BUCK, NANCY, M.A. Quadratic Reciprocity for the Rational Integers and the Gaussian Integers. (2010)
Directed by Dr. Brett Tangedal. pp.75

This thesis begins by giving a brief time line of the origins of Number Theory. It highlights the big theorems that have been constructed in this subject, along with the mathematicians who constructed them. The thesis, then, goes on to prove the Law of Quadratic Reciprocity for the Jacobi symbol. This includes proving Eisenstein's Lemma for the Jacobi symbol. Then, it is shown that Gauss's Lemma has an even greater generalization than Eisenstein's Lemma. Finally, this thesis shows the similarities between the rational integers and the Gaussian integers, including proving the Law of Quadratic Reciprocity for the Gaussian integers and constructing a similar version of Gauss's Lemma for the Gaussian integers.

QUADRATIC RECIPROCITY FOR THE RATIONAL INTEGERS AND THE GAUSSIAN INTEGERS

by

Nancy Buck

A Thesis Submitted to
the Faculty of The Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Arts

Greensboro
2010

Approved by

Committee Chair

APPROVAL PAGE

This thesis has been approved by the following committee of the
Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair ______________________________

Committee Members ______________________________

____

____
Date of Acceptance by Committee

____
Date of Final Oral Examination

ACKNOWLEDGMENTS

I would like to thank Dr. Brett Tangedal of the UNCG Math Department for advising me during the writing of this thesis. I would also like to thank Dr. Clifford Smyth and Dr. Dan Yasaki for being on my thesis committee. Finally, I would like to thank my parents for all of their support during this process.

TABLE OF CONTENTS

Page

CHAPTER

I. INTRODUCTION 1

II. QUADRATIC RECIPROCITY IN THE RATIONAL INTEGERS 13

III. QUADRATIC RECIPROCITY IN THE GAUSSIAN INTEGERS 38

BIBLIOGRAPHY 74

CHAPTER I
INTRODUCTION

During the 6th century B.C.E., the great mathematician Pythagoras formed a school in Croton, Italy, consisting of philosophers and mathematicians [2]. A famous tenet of this school was that "the world in all its aspects is governed by whole numbers and their relationships" [2]. Pythagoras and his students were fascinated with whole numbers, but the discovery that $\sqrt{2}$ is irrational (cannot be expressed as a ratio of two integers) caused much dismay [2]. Let $\mathbb{Z}$ denote the set of all integers, namely, $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$. We let $\mathbb{Z}^+$ denote the set of positive integers. From the point of view of multiplication, the most important subset of the integers is the set of prime numbers.

Definition 1. A *prime number* is any integer $n > 1$ whose only positive divisors are itself and 1.

It is easy to prove that every integer $n > 1$ is divisible by at least one prime number. Around 300 B.C. Euclid proved that there are infinitely many primes [8]. The proof, while short, was very clever on Euclid's part. Euclid reasoned as follows: Assume by way of contradiction that there are only finitely many prime numbers. Let $p_1 = 2 < p_2 = 3 < ... < p_r$ be the complete ordered list of all primes. Let $M = p_1 p_2 \cdots p_r + 1 > 1$ and let p be a prime dividing M. We have $p \notin \{p_1, p_2, ..., p_r\}$ since otherwise p would divide $M - p_1 p_2 \cdots p_r = 1$. Therefore, p is a prime not in the original (supposedly complete) list. This contradiction implies that there are infinitely many prime numbers.

Number Theory, loosely speaking, is the study of prime numbers and the special role they play among the integers. A few other definitions, crucial to the subject, are the following.

Definition 2. An integer $a \neq 0$ *divides* an integer b, if there exists an integer c such that $b = ca$. We denote this by $a \mid b$.

For example, $6 \mid 12$ since $12 = 2 \cdot 6$. However, 7 does not divide 10 and we use the notation $7 \nmid 10$ to denote this.

Definition 3. Let a and b be integers not both equal to zero. A *common divisor* of a and b is an integer c such that $c \mid a$ and $c \mid b$. If $d > 0$ is a common divisor of a and b and we have $c \leq d$ for every common divisor c of a and b, then d is said to be the *greatest common divisor* of a and b. We denote this by $(a, b) = d$.

Let $a = 12$ and $b = 18$. Since 6 is the largest integer that divides both 12 and 18, then $(12, 18) = 6$. Another example, with $a = 4$ and $b = 5$ gives $(4, 5) = 1$. When the greatest common divisor of two numbers is equal to 1, then those two numbers are said to be relatively prime. A basic fact, whose proof may be given in terms of an algorithm named in Euclid's honor, states that the greatest common divisor of a and b may be written as a linear combination of a and b. We state this more formally as follows.

Lemma 1. *Let a and b be integers not both equal to zero. There exist integers $s, t \in \mathbb{Z}$ such that $sa + tb = (a, b)$.*

While most people consider Pierre de Fermat (1601-1665) to be the founder of Modern Number Theory, Carl Friedrich Gauss (1777-1855) was the first mathematician to give this subject a systematic and rigorous foundation. In 1801, Gauss wrote *Disquisitiones Arithmeticae* which contains a proof of the Fundamental Theorem of Arithmetic. This theorem, which was first stated by Euclid, is the founding theorem of Modern Number Theory [6].

Theorem 1 (Fundamental Theorem of Arithmetic)**.** *Every positive integer greater than one can be written uniquely as a product of primes, with the prime factors in the product written in order of nondecreasing size.*

To prove this theorem, two small lemmas are needed:

Lemma 2. *If $a, b, c \in \mathbb{Z}^+$ such that $(a, b) = 1$ and $a \mid bc$, then $a \mid c$.*

Proof. Since $(a, b) = 1$, by Lemma 1 there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Now, multiply each side by c and the result is $acx + bcy = c$. Since $a \mid ac$ and $a \mid bc$, then $a \mid acx + bcy$. Therefore, $a \mid c$. $\square$

Lemma 3. *If $p \mid a_1 a_2 \cdots a_n$ where p is a prime and $a_1, a_2, ..., a_n \in \mathbb{Z}^+$, then there is an integer i with $1 \leq i \leq n$ such that $p \mid a_i$.*

Proof. Base case: $n = 1$ is trivial.
Induction Hypothesis: Given $k \geq 1$, assume that if $p \mid a_1 a_2 \cdots a_k$, where p is a prime, and $a_1, a_2, ..., a_k \in \mathbb{Z}^+$, then there is an integer i with $1 \leq i \leq k$ such that $p \mid a_i$. Now let $p \mid a_1 a_2 \cdots a_k a_{k+1}$ which implies that $p \mid (a_1 a_2 \cdots a_k)(a_{k+1})$. If $p \mid a_{k+1}$, then we are done. If $p \nmid a_{k+1}$, then $(p, a_{k+1}) = 1$ since p is a prime. Lemma 2 then implies that $p \mid a_1 a_2 \cdots a_k$ and by the Induction Hypothesis there is an integer i with $1 \leq i \leq k$ such that $p \mid a_i$ which means there is an integer i with $1 \leq i \leq k + 1$ such that $p \mid a_i$. Therefore, if $p \mid a_1 a_2 \cdots a_n$, where p is a prime and $a_1, a_2, ..., a_n \in \mathbb{Z}^+$, then there is an integer i with $1 \leq i \leq n$ such that $p \mid a_i$. $\square$

Based on the above, the following proof can be offered for the Fundamental Theorem of Arithmetic (Theorem 1). We first note that a positive integer $n > 1$ is said to be composite if it is not a prime. In this case, n may be written as a product $n = ab$, where $1 < a, b < n$.

Proof. Assume by way of contradiction that there exists a positive integer that cannot be written as a product of primes. Let n be the smallest integer for which this statement is true. Note that n must be composite since if n were a prime then n would be a (trivial) product of primes. Since n is composite, $n = ab$, with $1 < a < n$ and $1 < b < n$. Since $1 < a, b < n$ then both a and b may be written as a product of primes, which means that n can be written as a product of primes, giving a contradiction.

Now suppose that n had two different factorizations into primes such that: $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$, where $p_1, p_2, ..., p_s, q_1, q_2, ..., q_t$ are all primes and $p_1 \leq p_2 \leq ... \leq p_s$ and $q_1 \leq q_2 \leq ... \leq q_t$. Removing all common primes, this equation becomes possible: $p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$, so that all the primes on the right hand side of the equation are different from those primes on the left hand side of the equation and $u, v \geq 1$. By Lemma 3, $p_{i_1} \mid q_{j_k}$ from some k with $1 \leq k \leq v$, which is impossible since both p_{i_1} and q_{j_k} are primes that are different. Therefore, the prime factorization of n is unique. □

While the Greeks were interested in prime numbers, they really did not explore their potential much beyond Euclid's discoveries. It was not until the 1600's when Fermat began studying mathematics that prime numbers were more closely examined. Fermat spent a considerable amount of time completing the problems that the mathematician Diophantus posed in his book *Arithmetica*. It was from these roots that Fermat discovered two of his most famous results, known as Fermat's Little Theorem and Fermat's Last Theorem. Fermat developed his "little" Theorem around 1640 and claimed he had proof of it, but no indication of his method was ever found or published. The first known proof was given by Leibniz in an unpublished manuscript dating from about 1680 (see page 71 of [1]). The following crucial definition and extremely well-chosen notation was first introduced by Gauss in his *Disquisitiones Arthmeticæ*.

Definition 4. If $a, b, m \in \mathbb{Z}$ and $m \geq 2$, we say that *a is congruent to b modulo m* if $m \mid b - a$. This relation is written $a \equiv b \pmod{m}$.

For instance, $15 \equiv 4 \pmod{11}$ since $11 \mid 15 - 4$. With these definitions, we may now state Fermat's Little Theorem:

Theorem 2. *If p is a prime and p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.*

The first published proof of this theorem was due to Euler and appeared in 1736. The following refinement of Fermat's Little Theorem is also due to Euler.

Theorem 3. *If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m)$ is defined as the number of integers n such that $(n, m) = 1$ and $0 \leq n < m$.*

We follow the proof in [1] which requires a definition and lemma.

Definition 5. Let $m \geq 2$. A *reduced residue system modulo m* is a set of integers such that every number relatively prime to m is congruent modulo m to a unique element of the set. A reduced residue system modulo m has exactly $\phi(m)$ elements.

Lemma 4. *Let $r_1, r_2, ..., r_k$ be a reduced residue system modulo m where $k = \phi(m)$, and suppose $(a, m) = 1$. Then $ar_1, ar_2, ..., ar_k$ is a reduced residue system modulo m.*

Proof. First, we must show that no two elements of the sequence are congruent to each other modulo m. Suppose, by way of contradiction, that $ar_i \equiv ar_j \pmod{m}$ for some $i, j \in \mathbb{Z}$ with $i \neq j$. Since, $(a, m) = 1$, by Lemma 1 there exists $s, t \in \mathbb{Z}$ such that $sa + tm = 1$. Reducing modulo m, we have $sa \equiv 1 \pmod{m}$. Therefore, a has a multiplicative inverse s modulo m. So, we may multiply both sides of $ar_i \equiv ar_j \pmod{m}$ by s to get $r_i \equiv r_j \pmod{m}$, which is a contradiction since $r_1, r_2, ..., r_k$ is a reduced residue system modulo m.

Now, we must show that $(ar_i, m) = 1$ for $1 \leq i \leq k$. Since $(r_i, m) = 1$ and $(a, m) = 1$, then it follows that $(ar_i, m) = 1$. Therefore, $ar_1, ar_2, ..., ar_k$ is a collection of k incongruent integers modulo m, each of which is relatively prime to m, so by Definition 5, $ar_1, ar_2, ..., ar_k$ is a reduced residue system modulo m. $\square$

We are now able to prove Theorem 3 by following the proof on page 76 of [1].

Proof. Let $r_1, r_2, ..., r_{\phi(m)}$ be a reduced residue system modulo m. By Lemma 4, for $a \in \mathbb{Z}$ and $(a, m) = 1$, $ar_1, ar_2, ..., ar_{\phi(m)}$ is also a reduced residue system modulo m. Since both $r_1, r_2, ..., r_{\phi(m)}$ and $ar_1, ar_2, ..., ar_{\phi(m)}$ are reduced residue systems modulo m, we have $ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$ which implies that $a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$. Since each r_i is relatively prime to m, each r_i has a multiplicative inverse modulo m, and we may therefore cancel all of these to give $a^{\phi(m)} \equiv 1 \pmod{m}$. $\square$

As an example of Theorem 3, let $a = 7$ and $m = 6$. We have $(7, 6) = 1$ and $\phi(6) = 2$ since 1 and 5 are the only nonnegative integers less than 6 and relatively prime to 6. Note that $7^2 \equiv 1 \pmod{6}$. The proof of Fermat's Little Theorem follows directly from Theorem 3. If $m = p$ is a prime number in Theorem 3 and $p \nmid a$, which implies $(a, p) = 1$, then Theorem 2 is an immediate corollary of Theorem 3 since $\phi(p) = p - 1$.

Fermat's Last Theorem was stated in 1637, but not proved until 1995 by Andrew Wiles. Fermat's Last Theorem states that no 3 positive integers a, b, c can satisfy the equation $a^n + b^n = c^n$ for any $n > 2$. While this theorem has little importance to this thesis, the effort in trying to prove this theorem led to other branches of mathematics such as algebraic number theory in the 19th Century. However, there is another theorem of Fermat which is relevant to the purposes of this thesis.

Theorem 4. *Let p be an odd prime in $\mathbb{Z}$. Then $p = a^2 + b^2$ for integers a and b if and only if $p \equiv 1 \pmod 4$.*

The proof of this theorem becomes simple with the use of the first part of Quadratic Reciprocity and a theorem of Dirichlet which will be discussed in Chapter 3.

Before considering Euler and his advancements in Number Theory, specifically advancements of Quadratic Reciprocity, which shall be discussed in Chapter 2, another definition must be provided.

Definition 6. Let $a, m \in \mathbb{Z}$ and $m > 1$. If $(a, m) = 1$, a is called a *quadratic residue modulo m* if the congruence $x^2 \equiv a \pmod m$ has a solution $x \in \mathbb{Z}$. Otherwise, a is called a *quadratic nonresidue modulo m*.

Fermat's work led Euler to look at prime numbers of the form $x^2 + ay^2$, where $x, y \in \mathbb{Z}^+$ and $a \in \mathbb{Z}\backslash\{0\}$, and all of the prime divisors of such numbers [2]. In 1744, Euler published a paper which showed many of the exhaustive calculations he performed for this problem [2]. He was able to give proofs for the nontrivial prime divisors of numbers of the form $x^2 + ay^2$ where $a = 1, \pm 2, 3$, but was never able to complete a general proof to show the non-trivial prime divisors $p = x^2 + ay^2$ are the odd primes for which $-a$ is a nonzero quadratic residue modulo p [2]. In his work with prime numbers, Euler gave us another important theorem called Euler's Criterion:

Theorem 5 (Euler's Criterion)**.** *Let p be an odd prime and a an integer not divisible by p. The quantity $a^{(p-1)/2}$ is congruent to either 1 or -1 modulo p; a is a quadratic* *residue modulo p if and only if* $a^{(p-1)/2} \equiv 1 \pmod{p}$*.*

For example, if $p = 7$ and $a = 4$, then $4^{(7-1)/2} = 64 \equiv 1 \pmod{7}$. Therefore, by Theorem 5, 4 should be a quadratic residue modulo 7. Therefore, the congruence $x^2 \equiv 4 \pmod{7}$ should have a solution, which it does, namely $x = 2$ or $x = 5$. This is another theorem which can be easily proved by using a theorem due to Dirichlet.

Euler's successor at the Academy of Sciences in Berlin was Lagrange [2]. Lagrange used both Fermat's and Euler's work on the prime divisors of $x^2 + ay^2$ in the late 18th Century [2]. He realized the need to look at the more general quadratic form $ax^2 + bxy + cy^2$ and was able to take the problem much further than his predecessors [2]. He also developed a proof for the long standing problem that every positive integer could be written as the sum of four integer squares [2]. In 1782, Lagrange took notice of a young mathematician Legendre, who further advanced number theory, especially in the subject of quadratic reciprocity [2]. During the course of Legendre's study, he created a symbol now named in his honor.

Definition 7. Let p be an odd prime and assume that a is an integer such that $(p, a) = 1$. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } \; x^2 \equiv a \pmod{p} \quad \text{has a solution } x \in \mathbb{Z}. \\ -1 & \text{if } \; \text{there is no such solution.} \end{cases}$$

The Legendre symbol can be computed by using Euler's Criterion. For example, $\left(\frac{8}{11}\right) = -1$ since $8^{(11-1)/2}$ is not congruent to 1 (mod 11). The Legendre symbol has three important properties shown in the next theorem.

Theorem 6. *Let p be an odd prime and let* $a, b \in \mathbb{Z}$ *be such that* $(p, a) = (p, b) = 1$*.*

1. $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$*.*

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

3. If $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Proof. The first part is a direct result of Euler's Criterion since $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue modulo p and $\left(\frac{a}{p}\right) = -1$ if a is a quadratic nonresidue modulo p.

The second part is a direct result of the first part since

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Since the two quantities $\left(\frac{ab}{p}\right)$ and $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ are either 1 or -1, then either $p \mid -2$, $p \mid 0$, or $p \mid 2$. The fact that p is an odd prime means $p \nmid 2$, so the only possibility is $p \mid 0$ which implies $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Let $a \equiv b \pmod{p}$. This means if $x^2 \equiv a \pmod{p}$ has a solution, then $x^2 \equiv b \pmod{p}$ has a solution. If $x^2 \equiv a \pmod{p}$ does not have a solution, then $x^2 \equiv b \pmod{p}$ does not have a solution. Therefore, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. □

In working with his new symbol, Legendre tried to prove the Law of Quadratic Reciprocity which states:

Theorem 7. *Let p and q be distinct odd primes, then*

1. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

2. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

3. $\left(\frac{q}{p}\right) = (-1)^{[(q-1)(p-1)]/4}\left(\frac{p}{q}\right)$.

The proof of Theorem 7 will be discussed in Chapter 2. Unfortunately, Legendre was unable to prove this theorem. In *Disquistiones Arithmeticæ*, Gauss gave two proofs for the Law of Quadratic Reciprocity [6]. Then, in 1808 he developed two more proofs and two additional proofs in 1817 [6]. While Quadratic Reciprocity was obviously one of Gauss's favorite topics, he started a correspondence with another prominent mathematician named Dirichlet. Gauss and Dirichlet discussed biquadratic reciprocity, but they were not able to prove it. However, Dirichlet, in thinking of biquadratic reciprocity, was able to prove that Quadratic Reciprocity works for the Gaussian integers as well as the rational integers which will be discussed in Chapter 3. As mentioned before, Dirichlet discovered a nice theorem which leads to simplified proofs to some of the most prominent theorems in elementary number theory. Before stating that theorem, however, there is an important Lemma that Dirichlet needed in order to prove his theorem.

Lemma 5. *Let p be an odd prime and suppose $p \nmid a$. If $\left(\frac{a}{p}\right) = 1$, there are exactly two incongruent solutions $x \in \mathbb{Z}$ modulo p to $x^2 \equiv a \pmod{p}$.*

Proof. Since $\left(\frac{a}{p}\right) = 1$, there has to be a solution $b \in \mathbb{Z}$ to the congruence $x^2 \equiv a \pmod{p}$. In fact there has to be at least two incongruent solutions modulo p since if $b^2 \equiv a \pmod{p}$, then $(-b)^2 \equiv a \pmod{p}$ and b is not congruent to $-b$ modulo p since $p \neq 2$. Now $x^2 \equiv a \equiv b^2 \pmod{p}$, so $p \mid x^2 - b^2$ which implies $p \mid (x-b)(x+b)$. Since p is prime, $p \mid (x-b)$ or $p \mid (x+b)$. Therefore, by Definition 4, $x \equiv b \pmod{p}$ or $x \equiv -b \pmod{p}$, so there are exactly two incongruent solutions modulo p to the congruence $x^2 \equiv a \pmod{p}$. □

We are now able to state the following theorem by Dirichlet:

Theorem 8. *Let p be an odd prime, and suppose $1 \leq a \leq p-1$.*

If $\left(\frac{a}{p}\right) = -1$*, then* $(p-1)! \equiv a^{(p-1)/2} \pmod{p}$*. If* $\left(\frac{a}{p}\right) = 1$*, then* $(p-1)! \equiv -[a^{(p-1)/2}] \pmod{p}$*.*

Proof. We follow the proof in [1]. If $1 \leq m \leq p-1$, then there exists a unique s with $1 \leq s \leq p-1$ such that $ms \equiv 1 \pmod{p}$. Now let $n \in \mathbb{Z}$ be the unique integer with $1 \leq n \leq p-1$ such that $n \equiv sa \pmod{p}$. By multiplying the congruence by m, we are left with $mn \equiv msa \pmod{p}$ which implies $mn \equiv a \pmod{p}$. Call m and n corresponding numbers. If $\left(\frac{a}{p}\right) = -1$, then $m \neq n$ since $x^2 \equiv a \pmod{p}$ has no solution. Therefore, the numbers between 1 and $p-1$ can be paired off into $(p-1)/2$ distinct corresponding pairs, the product of each pair being congruent to a modulo p. By multiplying one side of these congruences, the result will be $(p-1)!$ and by multiplying the other side of these congruences, the result will be $a^{(p-1)/2}$. Therefore, $(p-1)! \equiv a^{(p-1)/2} \pmod{p}$.

If $\left(\frac{a}{p}\right) = 1$, then $x^2 \equiv a \pmod{p}$ is solvable. This means that there is a solution b such that $1 \leq b \leq p-1$. By Lemma 5, the only other solution in this range is $p-b$. We can arrange the remaining $p-3$ numbers between 1 and $p-1$ into corresponding pairs, the product of each pair being congruent to a modulo p. The product of these congruences will be congruent to $a^{(p-3)/2}$ modulo p. The product of b and $p-b$ will be congruent to $-a$ modulo p, so $(p-1)! \equiv (-a)(a)^{(p-3)/2} \equiv -[a^{(p-1)/2}] \pmod{p}$. □

For example, if $p = 7, a = 6$, then $\left(\frac{a}{p}\right) = -1$, and there are three different distinct pairs that make the following congruences: $1 \cdot 6 \equiv 6 \pmod{7}$, $2 \cdot 3 \equiv 6 \pmod{7}$, and $4 \cdot 5 \equiv 6 \pmod{7}$. If those three congruences are multiplied together, then the final congruence is $6! \equiv 6^3 \pmod{7}$, which is true. Now, let $p = 7, a = 2$ which means $\left(\frac{a}{p}\right) = 1$, and there are three congruences as follows: $1 \cdot 2 \equiv 2 \pmod{7}$, $3 \cdot 4 \equiv -2$

(mod 7) since $3^2 \equiv 2 \pmod 7$, and $5 \cdot 6 \equiv 2 \pmod 7$. Multiplying these three congruences together gives $6! \equiv -[2^3] \pmod 7$. As stated before, this theorem makes proving important theorems of number theory easy.

Consider Wilson's Theorem:

Theorem 9 (Wilson's Theorem)**.** *If p is a prime, then* $(p-1)! \equiv -1 \pmod p$.

Proof. If $p = 2$, then $(2-1)! = 1 \equiv -1 \pmod 2$. If p is odd, let $a = 1$ in Theorem 8. Obviously, $\left(\frac{1}{p}\right) = 1$, so $(p-1)! \equiv -[1^{(p-1)/2}] \pmod p$ which means $(p-1)! \equiv -1 \pmod p$. $\square$

Bringing together both Dirichlet's and Wilson's Theorems makes proving Euler's Criterion (Theorem 5) rather simple. Assume $\left(\frac{a}{p}\right) = 1$. Then, by Wilson and Dirichlet $-1 \equiv (p-1)! \equiv -[a^{(p-1)/2}] \pmod p$, so $a^{(p-1)/2} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$. Now assume $\left(\frac{a}{p}\right) = -1$. By Wilson and Dirichlet $-1 \equiv (p-1)! \equiv a^{(p-1)/2} \pmod p$, so $a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p$. This proves Euler's Criterion. $\square$

In addition to the works of Fermat and Gauss, there is another mathematician who is important in the field of Quadratic Reciprocity. In 1844, Eisenstein published two proofs of Quadratic Reciprocity [6]. One of those proofs will be discussed in Chapter 2.

CHAPTER II
QUADRATIC RECIPROCITY IN THE RATIONAL INTEGERS

In Chapter III, we will be working with a special set of numbers known as the "Gaussian integers". For clarity, we refer to the elements of $\mathbb{Z}$ as the rational integers. In most elementary number theory textbooks there is a proof given of the law of quadratic reciprocity due to Gauss based on Gauss's Lemma [3].

Definition 8. Let p be an odd prime. The set of *least residues modulo* p is $S = \{-(p-1)/2, -(p-3)/2, ..., -1, 1, 2, ..., (p-1)/2\}$.

For example, if $m = 4$ and $p = 7$, then the least residue modulo p of m would be -3.

Lemma 6 (Gauss's Lemma)**.** *If p is an odd prime and $m \in \mathbb{Z}$ is such that $p \nmid m$, then $\left(\frac{m}{p}\right) = (-1)^{\mu}$, where μ is the number of negative elements in the set of least residues modulo p of the integers $\{m, 2m, 3m, ..., ((p-1)/2)m\}$.*

By Gauss's Lemma, the Legendre symbol $\left(\frac{4}{7}\right)$ is equal to $(-1)^2 = 1$ since the least residues modulo 7 of 4, 8, and 12 are -3, 1, and -2, respectively.

In this chapter, we will prove the law of quadratic reciprocity in a more general form than that given in Chapter I, replacing Legendre symbols by the more flexible symbols defined in 1837 by Jacobi. We will for the most part follow the work of Eisenstein in this chapter. Eisenstein was a brilliant disciple of Gauss who provided many new insights into the reciprocity laws of number theory extending beyond the epic-making work of Gauss. Gauss's lemma may be slightly reformulated to apply to Jacobi symbols instead of just Legendre symbols and we will find that all of Eisenstein's ideas are also easily extended in this way as well.

Definition 9. Let $m, n \in \mathbb{Z}$ be such that $(m, n) = 1$ and $n = p_1 p_2 \cdots p_s$ is an odd integer greater than 1, where each p_i is an odd prime (we do not assume these primes are necessarily distinct among themselves). Then the *Jacobi symbol* is defined by $\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right) \cdots \left(\frac{m}{p_s}\right)$, where the symbols on the right side of the equation are Legendre symbols.

The Jacobi symbol shares many properties with the Legendre symbol. The following proposition will be useful in Chapter III.

Proposition 1. *Let n be an odd integer greater than one. If a and b are rational integers such that $(n, a) = (n, b) = 1$, then the following two properties hold for the Jacobi symbol.*

1. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

2. *If* $a \equiv b \pmod{n}$, *then* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

Proof. These two properties are easily deduced from parts 2 and 3, respectively, of Theorem 6 combined with the definition of the Jacobi symbol. □

An analogue to part 1 of Theorem 6 will be derived below in Lemma 9. Using the Jacobi symbol has the advantage that it allows the bottom number in the symbol to be any odd integer greater than one rather than just an odd prime. However, it should be noted that even if the Jacobi symbol is equal to 1, the numerator is not necessarily a quadratic residue with respect to the denominator. An example of this phenomenon is the following: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, and yet 2 is not a quadratic residue modulo 15. If the Jacobi symbol is equal to -1, then it is true that the numerator is a quadratic nonresidue with respect to the denominator [10].

Eisenstein was able to formulate another version of Gauss's Lemma called Eisenstein's Lemma that is often easier to apply. In order to state Eisenstein's Lemma, however, we need to define some preliminary notation. Let E denote the set of all positive even integers. Given an odd integer $n > 1$, let $E_n = \{a \in E \mid a < n\}$. If S is any non-empty subset of integers and $m \in \mathbb{Z}$, we will use the notation mS to denote the set $\{ms \mid s \in S\}$. As an example, $2E_7 = \{4, 8, 12\}$. Finally, let $[mE_n]_n$ denote the set of all non-negative remainders of the elements of the set mE_n upon division by n. For example, $[2E_7]_7 = \{4, 1, 5\}$.

Lemma 7 (Eisenstein's Lemma)**.** *Let $n > 1$ be an odd integer and m an integer such that $(m, n) = 1$. Then the Jacobi symbol $\left(\frac{m}{n}\right)$ is given by $\left(\frac{m}{n}\right) = (-1)^{\sum r}$, with summation over all $r \in [mE_n]_n$.*

Proof. We follow the proof in [3]. In order to prove Lemma 7, we need to set up some preliminary notation. Let $d > 1$ be an odd integer such that $d \mid n$, where $n = p_1^{n_1} \cdots p_t^{n_t}$, with each p_i an odd, distinct, rational prime. The set $E(d)$ defined by $E(d) = \{b \in E \mid 1 < b < d \text{ and } (b, d) = 1\}$ plays an important role in what follows. The cardinality of $E(d)$ is $\phi(d)/2$. To see this, recall that $\phi(d)$ is the number of integers c such that $(c, d) = 1$ and $0 < c < d$. For every odd integer c, such that $0 < c < d$ and $(c, d) = 1$, the corresponding even integer $b = d - c$ satisfies the conditions $0 < b < d$ and $(b, d) = 1$ as well. This confirms that the number of elements in $E(d)$ is equal to $\phi(d)/2$ since the set $E(d)$ contains only even integers.

For any given $a \in E_n$, the greatest common divisor (a, n) is such that $1 \leq$

$(a, n) < n$ and $(a, n) \mid n$. We may therefore write (a, n) in the form n/d, for some d as defined in the previous paragraph. With this choice, $(n/d) \mid a$ and so there exists $b \in \mathbb{Z}$ such that $a = (n/d)b$. Since a is even and (n/d) is odd, this implies that b is even. Furthermore, $\frac{b}{d} = \frac{a}{n}$, and since $a < n$ by assumption, we conclude that $b < d$. Clearly $b > 0$, and so b is an even integer in the range $0 < b < d$. Since $(a, n) = (n/d)$, by Lemma 1 there exist integers $k, l \in \mathbb{Z}$ such that $ak + nl = (n/d)$. Substituting $(n/d)b$ for a in this equation and multiplying through by d gives $nbk + ndl = n$. Dividing this last equation by n gives $bk + dl = 1$, which establishes that $(b, d) = 1$ and finally that $b \in E(d)$. We conclude that if $a \in E_n$ satisfies $(a, n) = (n/d)$, then a is contained within the set $(n/d)E(d)$. We now prove conversely that if $a \in E_n$ is such that $a \in (n/d)E(d)$, then $(a, n) = (n/d)$. By assumption, $a = (n/d)b$ for some $b \in E(d)$. Since $b \in E(d)$, by definition $(b, d) = 1$ which implies there exist $k, l \in \mathbb{Z}$ such that $bk + dl = 1$. Multiplying through by (n/d) gives $(n/d)bk + nl = (n/d)$. Substituting a for $(n/d)b$ gives $ak + nl = (n/d)$. By definition, the positive integer (a, n) divides both a and n and so $(a, n) \mid (n/d)$. Since (n/d) is also positive, we see that $(a, n) \leq (n/d)$. Note that $(n/d) \mid n$ and $(n/d) \mid a$ by assumption. This shows that (n/d) is a common divisor of a and n and thus $(n/d) \leq (a, n)$ since (a, n) is the greatest common divisor of a and n. Combining with the previous inequality gives $(a, n) = (n/d)$. In conclusion, $a \in E_n$ satisfies $(a, n) = (n/d)$ if and only if $a \in (n/d)E(d)$. This implies in turn that the set E_n may be partitioned into disjoint subsets as follows:

$$E_n = \cup_{d|n}(n/d)E(d),$$

where d runs through all positive divisors of n and we set $E(1) = \emptyset$. Since this argument was somewhat technical, it is worth illustrating the partition of the set E_n just given with a concrete example. Assume that $n = 45 = 3^2 \cdot 5$. The set E_{45} contains 22 elements, namely, $E_{45} = \{2, 4, 6, ..., 44\}$. The positive divisors d of n

are $d = 1, 3, 5, 9, 15, 45$. We have $E(1) = \emptyset$, $E(3) = \{2\}$, $E(5) = \{2, 4\}$, $E(9) = \{2, 4, 8\}$, $E(15) = \{2, 4, 8, 14\}$, and $E(45) = \{2, 4, 8, 14, 16, 22, 26, 28, 32, 34, 38, 44\}$. Therefore, $(45/45)E(45) = E(45)$, $(45/15)E(15) = \{6, 12, 24, 42\}$, $(45/9)E(9) = \{10, 20, 40\}$, $(45/5)E(5) = \{18, 36\}$, and $(45/3)E(3) = \{30\}$. Clearly each element in E_{45} occurs exactly once in one of the sets $(45/d)E(d)$ as d ranges through the possible values $d = 1, 3, 5, 9, 15$, and 45.

The set E_n contains $(n-1)/2$ elements and we claim that the set $[mE_n]_n$ also has this many elements. To see this, assume that a_1 and a_2 are two distinct elements in E_n and write $ma_i = q_i n + r_i$ for $i = 1, 2$, where $0 \leq r_1, r_2 < n$. To prove the claim we must show that $r_1 \neq r_2$. If on the contrary $r_1 = r_2$, then $ma_1 \equiv ma_2 \pmod{n}$. Since $(m, n) = 1$, there exist $k, l \in \mathbb{Z}$ such that $km + ln = 1$ which implies $km \equiv 1 \pmod{n}$. Therefore $kma_1 \equiv kma_2 \pmod{n}$ or $a_1 \equiv a_2 \pmod{n}$, contradicting the fact that a_1 and a_2 are distinct in E_n and establishing the claim. If $\sum r$ denotes the sum over all $r \in [mE_n]_n$ and $\sum r_d$ denotes the sum over all $r_d \in [m(n/d)E(d)]_n$, we may conclude that

$$(-1)^{\sum r} = (-1)^{\sum_{d|n} (\sum r_d)}$$

given that $[mE_n]_n$ has the same cardinality as E_n and given the partition of the set E_n derived above.

We now fix an integer $d > 1$ such that $d \mid n$ (d is odd since n is odd). We claim that the set $(n/d)[mE(d)]_d$ is identical to the set $[m(n/d)E(d)]_n$ we encountered just above. To see that the first set is contained in the second, let $b \in E(d)$ and write $mb = qd + s$ with $0 \leq s < d$. By our definitions above, $s \in [mE(d)]_d$. Multiplying through by (n/d) gives $m(n/d)b = qn + (n/d)s$, where $0 \leq (n/d)s < n$. This shows that $(n/d)s \in [m(n/d)E(d)]_n$, verifying the first inclusion. To see that the second set is contained in the first, let $b \in E(d)$ and write $m(n/d)b = qn + t$ with $0 \leq t < n$. By our definitions above, $t \in [m(n/d)E(d)]_n$. A slight regrouping leads to $m(n/d)b - q(n/d)d = t$, which in turn implies that $(n/d)s = t$ for some $s \in \mathbb{Z}$. Since $0 \le t < n$, we see that $0 \le (n/d)s < n$ or $0 \le s < d$. It remains to prove that $s \in [mE(d)]_d$. From above, $m(n/d)b = q(n/d)d + (n/d)s$. Canceling (n/d) gives $mb = qd + s$ and since $0 \le s < d$ we see that $s \in [mE(d)]_d$. Since this set equality proof is again somewhat technical, we illustrate the ideas involved with a concrete example. Assume that $n = 45$, as before, and let $m = 7$ and $d = 15$. We have $7E(15) = \{14, 28, 56, 98\}$ and so $[7E(15)]_{15} = \{14, 13, 11, 8\}$ or $(n/d)[mE(d)]_d = \{42, 39, 33, 24\}$. On the other hand, $7 \cdot 3E(15) = \{42, 84, 168, 294\}$ which implies that $[m(n/d)E(15)]_{45} = \{42, 39, 33, 24\}$. We conclude from the above set equality that each element $r_d \in [m(n/d)E(d)]_n$ may be written uniquely in the form $r_d = (n/d)s_d$ for some $s_d \in [mE(d)]_d$. Since (n/d) is odd (n being odd), we have $r_d \equiv s_d \pmod 2$ and therefore

$$(-1)^{\sum r} = (-1)^{\sum_{d|n}(\sum s_d)},$$

where again $\sum r$ denotes the sum over all $r \in [mE_n]_n$ and $\sum s_d$ denotes the sum over all $s_d \in [mE(d)]_d$.

We need two further lemmas in order to complete the proof of Lemma 7.

Lemma 8. *Let $d > 1$ be an odd integer and assume that m is an integer such that $(m, d) = 1$. We then have $m^{\phi(d)/2} \equiv (-1)^{\sum s_d} \pmod d$, with summation over all $s_d \in [mE(d)]_d$.*

Proof. We follow the proof in [3] which goes back to Eisenstein [12]. Let $b_1, ..., b_{\phi(d)/2}$ denote the elements of $E(d)$ and write $mb_i = q_i d + s_i$ with $0 \le s_i < d$ for $i = 1, ..., \phi(d)/2$. Note that $\{s_1, ..., s_{\phi(d)/2}\} = [mE(d)]_d$. If $c \in \mathbb{Z}^+$ is a common divisor of d and s_i for some $i \in \{1, ..., \phi(d)/2\}$, then $c \mid mb_i$ as well; however, m and b_i are both relatively prime to d so that $(mb_i, d) = 1$ and therefore $c = 1$. This implies that $(s_i, d) = 1$ for $i = 1, ..., \phi(d)/2$ and furthermore that each s_i is nonzero since $d > 1$.

We also claim that $s_i \neq s_j$ when $1 \leq i < j \leq \phi(d)/2$. If, on the contrary, $s_i = s_j$ for $i \neq j$, then $mb_i \equiv mb_j \pmod{d}$. Since $(m, d) = 1$, m has a multiplicative inverse modulo d and so $b_i \equiv b_j \pmod{d}$ for $i \neq j$. This is in contradiction to our definition of the set $E(d)$. Defining the new set $S = \{(-1)^{s_i} \cdot s_i \mid i = 1, ..., \phi(d)/2\}$, we note from above that this set contains $\phi(d)/2$ distinct integers that are all relatively prime to d. We now wish to show that the set $[S]_d$ also contains $\phi(d)/2$ distinct elements and that $[S]_d = E(d)$. We first recall the definition $E(d) = \{b \in E \mid 1 < b < d \text{ and } (b, d) = 1\}$ and that this set contains exactly $\phi(d)/2$ elements. If we show that $[S]_d \subseteq E(d)$ and that $[S]_d$ contains $\phi(d)/2$ distinct elements then the set equality $[S]_d = E(d)$ follows immediately. We first verify the set inclusion $[S]_d \subseteq E(d)$. If a given s_i is even, then $(-1)^{s_i} \cdot s_i = s_i \in [S]_d$ and $s_i \in E(d)$ as well since $1 < s_i < d$ and $(s_i, d) = 1$. If a given s_i is odd, then the number t_i defined by $(-1)^{s_i} \cdot s_i = -s_i = (-1)d + t_i$ is the corresponding element in $[S]_d$. Note that $0 < t_i < d$ and that t_i is even since d and s_i are both odd. We also have $(t_i, d) = 1$ since $(s_i, d) = 1$ and we conclude that $t_i \in E(d)$ and therefore $[S]_d \subseteq E(d)$. We next verify that $[S]_d$ contains $\phi(d)/2$ distinct elements. Assume that $1 \leq i < j \leq \phi(d)/2$. If s_i and s_j are both even then $s_i, s_j \in [S]_d$ and we already proved that $s_i \neq s_j$ above. If s_i and s_j are both odd, then $d - s_i = t_i$ and $d - s_j = t_j$ are both in $[S]_d$ and $t_i \neq t_j$ since $s_i \neq s_j$. If s_i is even and s_j is odd then s_i and $t_j = d - s_j$ are the corresponding elements in $[S]_d$. If we did have $s_i = t_j$, then $d = s_i + s_j = mb_i - q_i d + mb_j - q_j d$, which implies that $d \mid m(b_i + b_j)$. Since $(d, m) = 1$, we see in turn that $d \mid (b_i + b_j)$. Recall that $1 < b_i, b_j < d$ and so $1 < b_i + b_j < 2d$. Since $(b_i + b_j)$ is a multiple of d we must have $d = b_i + b_j$, but this is a contradiction since b_i and b_j are both even and d is odd. We conclude in this case that $s_i \neq t_j$. A similar argument holds when s_i is odd and s_j is even, demonstrating finally that $[S]_d$ contains $\phi(d)/2$ distinct elements and that $[S]_d = E(d)$. A concrete example helps clarify the proof. If $m = 7$ and

$d = 15$, then $[7E(15)]_{15} = \{14, 13, 11, 8\}$, as we saw in a previous example. The set S defined above is then equal to $S = \{14, -13, -11, 8\}$ and so $[S]_{15} = \{14, 2, 4, 8\}$, which coincides with $E(15)$.

The remainder of the proof follows with relative ease given that $[S]_d = E(d)$. An immediate consequence is the congruence

$$\prod_{i=1}^{\phi(d)/2} [(-1)^{s_i} \cdot s_i] \equiv \prod_{i=1}^{\phi(d)/2} b_i \pmod{d}.$$

The congruence

$$\prod_{i=1}^{\phi(d)/2} [(-1)^{s_i} \cdot mb_i] \equiv \prod_{i=1}^{\phi(d)/2} [(-1)^{s_i} \cdot s_i] \pmod{d}$$

follows immediately from the equations $mb_i = q_i d + s_i$ for $i = 1, ..., \phi(d)/2$. Combining these two congruences gives

$$m^{\phi(d)/2} \cdot (-1)^{\sum_{i=1}^{\phi(d)/2} s_i} \cdot \prod_{i=1}^{\phi(d)/2} b_i \equiv \prod_{i=1}^{\phi(d)/2} b_i \pmod{d}.$$

Since $\{s_1, ..., s_{\phi(d)/2}\} = [mE(d)]_d$, we have $\sum_{i=1}^{\phi(d)/2} s_i = \sum s_d$, with the second summation taken over all $s_d \in [mE(d)]_d$. Each $b_i \in E(d)$ is relatively prime to d *by definition* and therefore $(\prod_{i=1}^{\phi(d)/2} b_i, d) = 1$. This implies that the quantity $\prod_{i=1}^{\phi(d)/2} b_i$ has a multiplicative inverse modulo d which justifies cancellation in the last congruence above to obtain

$$m^{\phi(d)/2} \cdot (-1)^{\sum s_d} \equiv 1 \pmod{d}$$

(it is probably only now that one fully appreciates why the set $E(d)$ was introduced and defined as it was). Since the quantity $(-1)^{\sum s_d}$ is either 1 or -1, we may multiply both sides of the congruence by it to finally obtain

$$m^{\phi(d)/2} \equiv (-1)^{\sum s_d} \pmod{d}.$$

$\square$

Lemma 9. *Let $d > 1$ be an odd integer and assume that m is an integer such that $(m, d) = 1$. If $d = p^k$ (p an odd prime), then $m^{\phi(d)/2} \equiv \left(\frac{m}{p}\right) \pmod{d}$, where $\left(\frac{m}{p}\right)$ is the Legendre symbol. If d is not a prime power, then $m^{\phi(d)/2} \equiv 1 \pmod{d}$.*

Proof. We follow the proof in [3]. Let $d = p^k$, where p is an odd prime and $k \geq 1$. If $k = 1$, then $d = p$ and $\phi(d) = p - 1$ and Euler's criterion (Theorem 5) gives $m^{\phi(d)/2} \equiv \left(\frac{m}{p}\right) \pmod{p}$, which completes the proof in this case. We now assume that $k > 1$. If $l \geq 1$ and $a \equiv b \pmod{p^l}$, then $a^p \equiv b^p \pmod{p^{l+1}}$ by the binomial theorem (see Lemma 3 on page 42 of [10] for a detailed proof). For example, given $m^{(p-1)/2} \equiv \left(\frac{m}{p}\right) \pmod{p}$, we obtain $m^{(1/2)(p-1)p} \equiv \left(\frac{m}{p}\right)^p \pmod{p^2}$ when $l = 1$. Applying this same step repetitively for $l = 2, ..., k-1$ yields finally $m^{(1/2)(p-1)p^{k-1}} \equiv \left(\frac{m}{p}\right)^{p^{k-1}} \pmod{p^k}$. The exponent on the left hand side may be rewritten as $(1/2)\phi(p^k)$ (see page 77 of [1]), or simply $\phi(d)/2$. The Legendre symbol $\left(\frac{m}{p}\right)$ is equal to 1 or -1 and thus $\left(\frac{m}{p}\right)^{p^{k-1}} = \left(\frac{m}{p}\right)$ since p^{k-1} is an odd integer. This completes the proof when $d = p^k$.

We now assume that d is not a prime power. The factorization of d into distinct prime powers then has the form $d = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, where $s \geq 2$ and each exponent k_i is positive (all primes appearing here are odd). As we saw above, $m^{(1/2)\phi(p_i^{k_i})} \equiv \pm 1 \pmod{p_i^{k_i}}$ for $i = 1, ..., s$. Since $p_1, p_2, ..., p_s$ are all distinct from each other, and the Euler ϕ-function is multiplicative (see pages 76-77 of [1]), we have $\phi(d) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_s^{k_s})$. The integer $\phi(p_j^{k_j})$ is even (see page 90 of [1]) for each $j \in \{1, ..., s\}$ and therefore $m^{(1/2)\phi(d)} \equiv (\pm 1)^{v_i} \pmod{p_i^{k_i}}$ for $i = 1, ..., s$, where each v_i is even. This implies that $p_i^{k_i} \mid m^{(1/2)\phi(d)} - 1$ for $i = 1, ..., s$ and since

$d = p_1^{k_1} \cdots p_s^{k_s}$ is a factorization of d into relatively prime powers we conclude (see Theorem 1.10(ii) on page 9 of [1]) that $d \mid m^{(1/2)\phi(d)} - 1$, completing the proof. $\square$

We are now ready to complete the proof of Eisenstein's Lemma (Lemma 7). Recall that m is a fixed integer relatively prime to the odd integer $n > 1$. We have seen above that we need to run through and consider in turn each $d > 1$ that divides n (note that m is relatively prime to each such d). Assume that the odd prime p divides n to exactly the $k \geq 1$ power. When $d = p^l$ $(1 \leq l \leq k)$, we may combine Lemmas 8 and 9 to conclude that $(-1)^{\sum s_{p^l}} \equiv \left(\frac{m}{p}\right) \pmod{p^l}$, where $\sum s_{p^l}$ denotes the sum over all $s_{p^l} \in [mE(p^l)]_{p^l}$. Since both sides of this congruence are either 1 or -1 and $p^l > 2$, we see that $(-1)^{\sum s_{p^l}} = \left(\frac{m}{p}\right)$. Since the right hand side is independent of the exponent l, this implies that $\sum s_p \equiv \sum s_{p^l} \pmod 2$ for any integer l with $1 \leq l \leq k$. If $d > 1$ is a divisor of n and d is not a prime power, we may combine Lemmas 8 and 9 to conclude that $(-1)^{\sum s_d} \equiv 1 \pmod d$, where $\sum s_d$ denotes the sum over all $s_d \in [mE(d)]_d$. Since $d > 2$, we see that $(-1)^{\sum s_d} = 1$ and therefore the sum $\sum s_d$ is even in this case. Immediately before stating and proving Lemma 8, we derived the formula

$$(-1)^{\sum r} = (-1)^{\sum_{d|n} (\sum s_d)},$$

where $\sum r$ denotes the sum over all $r \in [mE_n]_n$. In order to finally show that the Jacobi symbol $\left(\frac{m}{n}\right)$ is given by $\left(\frac{m}{n}\right) = (-1)^{\sum r}$, we must evaluate the exponent $\sum_{d|n} (\sum s_d)$ modulo 2, which we are now in a position to do. The sum $\sum_{d|n}$ runs through all positive (necessarily odd) divisors d of n. If $d = 1$, there is no contribution to this sum. If $d > 1$ is not a prime power, we saw above that $\sum s_d$ is even and therefore may be ignored modulo 2. The only d of interest are the prime power divisors of n. Returning to our previous example, if $n = 45$, the positive divisors are $d = 1, 3, 5, 9, 15, 45$, but only $d = 3, 5$, and 9 make interesting contributions to the final answer. In summary,

$$\sum_{d|n} (\sum s_d) \equiv \sum_{l_1=1}^{n_1} (\sum s_{p_1^{l_1}}) + \cdots + \sum_{l_t=1}^{n_t} (\sum s_{p_t^{l_t}}) \pmod 2,$$

where $n = p_1^{n_1} \cdots p_t^{n_t}$. We saw above that $\sum s_{p_i} \equiv \sum s_{p_i^{l_i}} \pmod 2$ for $1 \leq i \leq t$ and $1 \leq l_i \leq n_i$ and so

$$\sum_{d|n} (\sum s_d) \equiv n_1 \sum s_{p_1} + \cdots + n_t \sum s_{p_t} \pmod 2.$$

The formula $(-1)^{\sum s_{p_i}} = \left(\frac{m}{p_i}\right)$ was derived just above and putting everything together leads to the following equations

$$\begin{aligned}(-1)^{\sum r} &= (-1)^{\sum_{d|n} (\sum s_d)} = [(-1)^{\sum s_{p_1}}]^{n_1} \cdots [(-1)^{\sum s_{p_t}}]^{n_t} \\ &= \left(\frac{m}{p_1}\right)^{n_1} \cdots \left(\frac{m}{p_t}\right)^{n_t} = \left(\frac{m}{n}\right),\end{aligned}$$

with the last equation being simply the definition of the Jacobi symbol. □

Having proved Eisenstein's Lemma for the Jacobi symbol (Lemma 7), we now state (Theorem 10 below) and prove the law of quadratic reciprocity for Jacobi symbols. We follow the proofs given in [3] and [4] which were directly inspired by Eisenstein's beautiful papers [12], [13]. The resemblance between Theorem 10 and Theorem 7 is remarkably close and clearly indicates that the Jacobi symbol is an extremely well chosen generalization of the Legendre symbol. Theorem 10 is the key to proving all other reciprocity laws discussed in this thesis and, in particular, Theorem 7 is an immediate corollary of it.

Theorem 10. *If m and n are odd integers each greater than 1 such that $(m, n) = 1$, then*

1. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

2. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

3. $\left(\frac{m}{n}\right) = (-1)^{[(m-1)(n-1)]/4}\left(\frac{n}{m}\right)$.

Proof. Part 1 is a direct consequence of Lemma 7. The integer $m = -1$ is relatively prime to the fixed odd integer $n > 1$. By Lemma 7, $\left(\frac{-1}{n}\right) = (-1)^{\sum r}$, with summation over all $r \in [(-1)E_n]_n$. This implies that $\left(\frac{-1}{n}\right) = (-1)^t$, where t is the number of odd integers contained in the set $[(-1)E_n]_n$. By definition, $(-1)E_n = \{-2, -4, ..., -(n-1)\}$ and therefore $[(-1)E_n]_n = \{n-2, n-4, ..., 1\}$. Since n is odd, every element in the set $[(-1)E_n]_n$ is odd and so $t = (n-1)/2$, completing the proof of part 1.

The second part of Theorem 10 is also a direct result of Lemma 7. Since n is an odd integer, either $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$ and $m = 2$ is relatively prime to n. By Lemma 7, $\left(\frac{2}{n}\right) = (-1)^t$, where t is the number of odd integers contained in the set $[2E_n]_n$. First assume that $n \equiv 1 \pmod 4$. The set E_n may be written as $E_n = \{2, ..., (n-1)/2\} \cup \{(n+3)/2, ..., (n-1)\}$, where each of the two subsets contains $(n-1)/4$ elements. The set $2E_n$ has the form $\{4, ..., (n-1)\} \cup \{(n+3), ..., 2(n-1)\}$ and therefore $[2E_n]_n = \{4, ..., (n-1)\} \cup \{(n+3)-n, ..., 2(n-1)-n\}$. Since n is odd, the elements of the first subset are all even and the elements of the second subset are all odd and so by Lemma 7, $\left(\frac{2}{n}\right) = (-1)^{(n-1)/4}$. Since $n \equiv 1 \pmod 4$, it follows that $n \equiv 1 \pmod 8$ or $n \equiv 5 \pmod 8$. If $n \equiv 1 \pmod 8$, then $n = 8k+1$ with $k \in \mathbb{Z}^+$, which implies that $\left(\frac{2}{n}\right) = (-1)^{(8k+1-1)/4} = (-1)^{2k} = 1 = (-1)^{(n^2-1)/8}$. If $n \equiv 5 \pmod 8$, then $n = 8k+5$ with k a nonnegative integer, which implies that $\left(\frac{2}{n}\right) = (-1)^{(8k+5-1)/4} = (-1)^{2k+1} = -1 = (-1)^{(n^2-1)/8}$.

We now consider the case where $n \equiv 3 \pmod 4$. If $n = 3$, then

$$\left(\frac{2}{3}\right) = -1 = (-1)^{(n^2-1)/8},$$

which covers this one special case. If $n > 3$, then E_n may be written as $E_n = \{2, ..., (n-3)/2\} \cup \{(n+1)/2, ..., (n-1)\}$, where the first subset contains $(n-3)/4$ elements and the second subset contains $(n+1)/4$ elements. The set $2E_n$ has the form $\{4, ..., (n-3)\} \cup \{(n+1), ..., 2(n-1)\}$ and therefore $[2E_n]_n = \{4, ..., (n-3)\} \cup \{(n+1)-n, ..., 2(n-1)-n\}$. Since n is odd, all of the elements of the first subset are even and all of the elements of the second subset are odd and so by Lemma 7, $\left(\frac{2}{n}\right) = (-1)^{(n+1)/4}$. Since $n \equiv 3 \pmod 4$, it follows that $n \equiv 3 \pmod 8$ or $n \equiv 7 \pmod 8$. If $n \equiv 3 \pmod 8$, then $n = 8k+3$ with $k \in \mathbb{Z}^+$, which implies that $\left(\frac{2}{n}\right) = (-1)^{(8k+3+1)/4} = (-1)^{2k+1} = -1 = (-1)^{(n^2-1)/8}$. If $n \equiv 7 \pmod 8$, then $n = 8k+7$ with k a nonnegative integer, which implies that $\left(\frac{2}{n}\right) = (-1)^{(8k+7+1)/4} = (-1)^{2k+2} = 1 = (-1)^{(n^2-1)/8}$, completing the verification of part 2 in all cases.

The third part of Theorem 10 is the most important and requires significantly more insight to prove. Eisenstein gave an elegant geometric argument in [12] for part three by counting lattice points in the X-Y plane in conjunction with a clever usage of his lemma and this method is followed in [3]. We will instead present an analytic proof due to Eisenstein [13] involving the trigonometric sine function. This proof lies deeper and Eisenstein in this same paper [13] gave a remarkable generalization of it to prove the law of biquadratic reciprocity, replacing the sine function by a special elliptic function discovered independently by Gauss and Abel known as the lemniscatic sine function.

To begin with, we will need the following lemma:

Lemma 10. *If m is a positive odd integer and w and y are any given nonzero complex numbers, then the following identity holds: $w^m - y^m = \prod_{k=0}^{m-1} (\zeta^k w - \zeta^{-k} y)$, where $\zeta = e^{2\pi i/m}$.*

Proof. The polynomial $z^m - 1$ has m distinct complex number roots and they are precisely the m numbers $1, \zeta, ..., \zeta^{m-1}$, implying that $z^m - 1 = \prod_{k=0}^{m-1} (z - \zeta^k)$. If we set $z = \frac{w}{y}$, then $\frac{w^m}{y^m} - 1 = \prod_{k=0}^{m-1} (\frac{w}{y} - \zeta^k)$, or $w^m - y^m = \prod_{k=0}^{m-1} (w - \zeta^k y)$, upon multiplication on both sides by y^m. Since m is odd, as k runs through the values $0, 1, ..., m-1$, then $-2k$ also runs through a complete system of residues modulo m. Since $\zeta^a = \zeta^b$ for any two integers $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{m}$, we find that

$$\begin{aligned} w^m - y^m = \prod_{k=0}^{m-1} (w - \zeta^{-2k} y) &= \prod_{k=0}^{m-1} \zeta^{-k} (\zeta^k w - \zeta^{-k} y) \\ &= \zeta^{-(1+2+\cdots+(m-1))} \prod_{k=0}^{m-1} (\zeta^k w - \zeta^{-k} y). \end{aligned}$$

Upon demonstrating that $\zeta^{-(1+2+\cdots+(m-1))} = 1$, or equivalently that the exponent is divisible by m, since $\zeta^m = 1$, the proof will be complete. The classic identity $1 + 2 + \cdots + (m-1) = [m(m-1)]/2$ is easily proved by induction. Since m is odd, $(m-1)/2$ is an integer, showing that the above exponent is equal to $m \cdot a$, $a \in \mathbb{Z}$, and thus is divisible by m. $\square$

We are ready to prove part three of Theorem 10. Let $m > 0$ be an odd integer. By Lemma 10, for all $w, y \in \mathbb{C} \backslash \{0\}$, $w^m - y^m = \prod_{k=0}^{m-1} (\zeta^k w - \zeta^{-k} y)$ where $\zeta = e^{2\pi i/m}$. Let $w = e^{ix}$ and $y = e^{-ix}$ for all $x \in \mathbb{R}$. By Lemma 10 and trigonometry we have

$$e^{ixm} - e^{-ixm} = \cos(mx) + i\sin(mx) - (\cos(-mx) + i\sin(-mx))$$
$$= \prod_{k=0}^{m-1}(\zeta^k e^{ix} - \zeta^{-k} e^{-ix}).$$

Further, combining like terms and replacing ζ with $e^{\frac{2\pi ik}{m}}$ we have the following equality:

$$2i\sin(mx) = \prod_{k=0}^{m-1}(e^{\frac{2\pi ik}{m}} e^{ix} - e^{\frac{-2\pi ik}{m}} e^{-ix}) = \prod_{k=0}^{m-1}(e^{\frac{2\pi ik+ixm}{m}} - e^{\frac{-2\pi ik-ixm}{m}}).$$

By using the same trigonometry identity again, we find the next equation:

$$2i\sin(mx) = \prod_{k=0}^{m-1}(e^{i\frac{2\pi k+xm}{m}} - e^{i\frac{-2\pi k-xm}{m}}) = \prod_{k=0}^{m-1} 2i\sin(x + \frac{2\pi k}{m}).$$

For the next equality, we were able to factor $(2i)^m$ out of the product and divide each side of the equation by $2i$ and get:

$$\sin(mx) = (2i)^{m-1}\prod_{k=0}^{m-1}\sin(x + \frac{2\pi k}{m}) = 2^{m-1}(-1)^{(m-1)/2}\prod_{k=0}^{m-1}\sin(x + \frac{2\pi k}{m}).$$

Finally, we separate the product into two different products, the first ranging from $1 \leq k \leq (m-1)/2$ and the second ranging from $(m+1)/2 \leq k \leq m-1$, resulting in this equation:

$$\sin(mx) = 2^{m-1}(-1)^{(m-1)/2}\sin(x)\prod_{k=1}^{(m-1)/2}\sin(x + \frac{2\pi k}{m})\prod_{k=(m+1)/2}^{m-1}\sin(x + \frac{2\pi k}{m}).$$

Since the sine function is periodic:

$$\sin(x + \frac{2k\pi}{m}) = \sin(x + \frac{2k\pi}{m} - 2\pi) = \sin(x - \frac{2\pi(k-m)}{m}).$$

Further, as k goes from $(m+1)/2$ to $m-1$, $m-k$ goes from $(m-1)/2$ to 1, meaning that $\sin(mx) = 2^{m-1}(-1)^{(m-1)/2}\sin(x)\prod_{k=1}^{(m-1)/2}\sin(x+\frac{2\pi k}{m})\sin(x-\frac{2\pi k}{m})$. Let $x = \frac{2\pi l}{n}$ where $l \in \mathbb{Z}$ for $1 \leq l \leq (n-1)/2$ where $n > 1$ is odd. This results in:

$$\sin(\frac{2\pi ml}{n}) = 2^{m-1}(-1)^{(m-1)/2}\sin(x)\prod_{k=1}^{(m-1)/2}\sin(\frac{2\pi l}{n}+\frac{2\pi k}{m})\sin(\frac{2\pi l}{n}-\frac{2\pi k}{m}),$$

and so

$$\prod_{l=1}^{(n-1)/2}\left(\frac{\sin(\frac{2\pi ml}{n})}{\sin(\frac{2\pi l}{n})}\right) =$$

$$2^{[(m-1)(n-1)]/2}(-1)^{(m-1)(n-1)/4}\sin(x)\prod_{l=1}^{(n-1)/2}\prod_{k=1}^{(m-1)/2}\sin\left(\frac{2\pi l}{n}+\frac{2\pi k}{m}\right)\sin\left(\frac{2\pi l}{n}-\frac{2\pi k}{m}\right). \tag{2.1}$$

We claim that the Jacobi symbol can be represented as:

$$\left(\frac{m}{n}\right) = \prod_{l=1}^{(n-1)/2}\left(\frac{\sin(\frac{2\pi ml}{n})}{\sin(\frac{2\pi l}{n})}\right) \tag{2.2}$$

To see this, we need to show that $\sin\left(\frac{2\pi l}{n}\right) \neq 0$. Since $1 \leq l \leq (n-1)/2$, by multiplying through by $2\pi/n$, we are left with $0 < \frac{2\pi l}{n} < \pi$. Since $\sin(\theta) > 0$ for $0 < \theta < \pi$, $\sin(\frac{2\pi l}{n}) > 0$. If $m = 1$, then the claim is true. Consider $m > 1$. Remember $E_n = \{2, 4, ..., n-1\} = \{2l \mid 1 \leq l \leq (n-1)/2\}$. For each l such that $1 \leq l \leq (n-1)/2$, divide $2lm$ by n which leads to the equation $2lm = q_l n + r_l$ for $0 < r_l < n$. Next, set $t_l = r_l$ when r_l is even and set $t_l = n - r_l$ when r_l is odd. Since n is odd and $r_l < n$, it is clear that $t_l \in E_n$ for each l with $1 \leq l \leq (n-1)/2$. Since $n \mid 2lm - r_l$, then for $1 \leq l \leq (n-1)/2$, $2lm \equiv r_l \equiv t_l \pmod{n}$ when r_l is even and $2lm \equiv -(n-r_l) \equiv -t_l \pmod{n}$ when r_l is odd. Define $\sigma_n(2l, m) \in \{-1, 1\}$ such that

$$2lm \equiv \sigma_n(2l, m) \cdot t_l \pmod{n} \tag{2.3}$$

where $1 \leq l \leq (n-1)/2$. From the previous congruences we have

$$\sigma_n(2l, m) = \begin{cases} 1 & \text{if } r_l \text{ is even,} \\ -1 & \text{if } r_l \text{ is odd.} \end{cases} \tag{2.4}$$

We need to show that $E_n = \{t_1, t_2, ..., t_{(n-1)/2}\}$. Since we know that $t_l \in E_n$ for each l with $1 \leq l \leq (n-1)/2$, it follows that $\{t_1, t_2, ..., t_{(n-1)/2}\} \subseteq E_n$. Since E_n has $(n-1)/2$ elements, we need to show that $E_n = \{t_1, t_2, ..., t_{(n-1)/2}\}$ is to show that all the t_1's are distinct. Assume that $1 \leq j < l \leq (n-1)/2$ for $j, l \in \mathbb{Z}$. We want to prove that $t_j \neq t_l$.

Case 1: Assume that r_l and r_j are both even. This means that $r_l = t_l$ and $r_j = t_j$. Assume by way of contradiction that $t_j = t_l$. Since we know $2lm \equiv t_l \pmod{n}$ and $2jm \equiv t_j \pmod{n}$, then $2jm \equiv 2lm \pmod{n}$ which implies $n \mid 2m(l-j)$. Since n is odd and $(n, m) = 1$, then $(n, 2m) = 1$, so $n \mid (l-j)$ which is a contradiction since $0 < l - j < n$, and so $t_j \neq t_l$.

Case 2: Assume that r_1 and r_j are both odd. This means that $n - r_l = t_l$ and $n - r_j = t_j$. Assume by way of contradiction that $t_j = t_l$. Since $2lm \equiv -t_l \pmod{n}$ and $2jm \equiv -t_j \pmod{n}$, then $2jm \equiv 2lm \pmod{n}$ which implies $n \mid 2m(l-j)$. Since n is odd and $(n, m) = 1$, then $(n, 2m) = 1$, so $n \mid l - j$ which is a contradiction since $0 < l - j < n$, and so $t_j \neq t_l$.

Case 3: Assume r_l is even and r_j is odd. This means that $r_l = t_l$ and $n - r_j = t_j$. Assume by way of contradiction that $t_j = t_l$. Since we know $2lm \equiv t_l \pmod{n}$ and $2jm \equiv -t_j \pmod{n}$, then $2lm \equiv -2jm \pmod{n}$ which implies $n \mid 2m(l+j)$. Since n is odd and $(n, m) = 1$, then $(n, 2m) = 1$, so $n \mid (l+j)$ which is a contradiction since $0 < l + j < n$, and so $t_j \neq t_l$. If r_1 is odd and r_j is even, the same argument occurs.

Therefore, all the t_l's are distinct which means that $E_n = \{t_1, t_2, ..., t_{(n-1)/2}\}$.

Recall that if $(m,n) = 1$, then $\left(\frac{m}{n}\right) \in \{-1, 1\}$. By Eisenstein's Lemma, $\left(\frac{m}{n}\right) = (-1)^{\sum_{l=1}^{(n-1)/2} r_l}$ since the $r_l \in [mE_n]_n$. By equation 2.4, we have the following equality

$$(-1)^{\sum_{l=1}^{(n-1)/2} r_l} = \prod_{l=1}^{(n-1)/2} \sigma_n(2l, m). \tag{2.5}$$

At this point, to prove equation (2.2) we need to show that

$$\prod_{l=1}^{(n-1)/2} \sigma_n(2l, m) = \prod_{l=1}^{(n-1)/2} \left\{ \frac{\sin\left(\frac{2\pi ml}{n}\right)}{\sin\left(\frac{2\pi l}{n}\right)} \right\} \tag{2.6}$$

The congruence in (2.3) can be written as the equation

$$2lm = \sigma_n(2l, m) \cdot t_l + b_l n$$

for each l with $1 \leq l \leq (n-1)/2$. Since $2lm$ and t_l are even and n is odd, this means that b_l must be even. We rewrite the equation with $b_l = 2a_l$ where $a_l \in \mathbb{Z}$ and multiply each side of the equation by $\frac{\pi}{n}$ to get the new equation

$$\frac{2\pi lm}{n} = \frac{\sigma_n(2l, m)\pi t_l}{n} + 2\pi a_l$$

for each l with $1 \leq l \leq (n-1)/2$. Taking the sine function of both sides you get the following equation

$$\sin\left(\frac{2\pi lm}{n}\right) = \sin\left(\frac{\sigma_n(2l, m)\pi t_l}{n}\right)$$

for each l with $1 \leq l \leq (n-1)/2$. This is true since $\sin(x + 2\pi a) = \sin(x)$ for all $a \in \mathbb{Z}$. Since the sine function is an odd function, $\sin(-x) = -\sin(x)$ for all $x \in \mathbb{R}$, so since $\sigma_n(2l,m) \in \{-1,1\}$ we can find the new equation

$$\sin\left(\frac{2\pi lm}{n}\right) = \sigma_n(2l,m)\sin\left(\frac{\pi t_l}{n}\right)$$

for each l with $1 \le l \le (n-1)/2$. Since $E_n = \{t_1, t_2, ..., t_{(n-1)/2}\}$, we can take the product over all l to get the following equality

$$\prod_{l=1}^{(n-1)/2} \sin\left(\frac{2\pi lm}{n}\right) = \prod_{l=1}^{(n-1)/2} \sigma_n(2l,m) \prod_{l=1}^{(n-1)/2} \sin\left(\frac{2l\pi}{n}\right).$$

Therefore, equation (2.6) holds.

By combining, equations (2.5) and (2.6), we can see that equation (2.2) is true when $(m,n) = 1$.

Since equation (2.2) is true, it is just a matter of trigonometry to prove part 3 of Theorem 10. By combining (2.1) and (2.2) we get the following equation

$$\left(\frac{m}{n}\right) = \prod_{l=1}^{(n-1)/2} \left(\frac{\sin\left(\frac{2\pi ml}{n}\right)}{\sin\left(\frac{2\pi l}{n}\right)}\right) = 2^{[(m-1)(n-1)]/2}(-1)^{(m-1)(n-1)/4}\sin(x)$$
$$\prod_{l=1}^{(n-1)/2}\prod_{k=1}^{(m-1)/2} \sin\left(\frac{2\pi l}{n} + \frac{2\pi k}{m}\right)\sin\left(\frac{2\pi l}{n} - \frac{2\pi k}{m}\right). \quad (2.7)$$

By symmetry, we can also write

$$\left(\frac{n}{m}\right) = \prod_{k=1}^{(m-1)/2} \left(\frac{\sin\left(\frac{2\pi nk}{m}\right)}{\sin\left(\frac{2\pi k}{m}\right)}\right) = 2^{[(n-1)(m-1)]/2}(-1)^{(n-1)(m-1)/4}\sin(x)$$
$$\prod_{k=1}^{(m-1)/2}\prod_{l=1}^{(n-1)/2} \sin\left(\frac{2\pi k}{m} + \frac{2\pi l}{n}\right)\sin\left(\frac{2\pi k}{m} - \frac{2\pi l}{n}\right). \quad (2.8)$$

Since the sine function is odd, we can rewrite $\sin(\frac{2\pi k}{m} - \frac{2\pi l}{n})$ as $-\sin(-\frac{2\pi k}{m} + \frac{2\pi l}{n})$ in equation (2.8) which leads to the final result that

$$\left(\frac{m}{n}\right) = (-1)^{[(m-1)(n-1)]/4}\left(\frac{n}{m}\right).$$

This is true, since by changing that last sine function in (2.8), both equations (2.7) and (2.8) are exactly the same except for a factor of $(-1)^{[(m-1)(n-1)]/4}$. This proves Quadratic Reciprocity for the Jacobi symbol (Theorem 10). □

While we have proved Quadratic Reciprocity for the rational integers in this chapter, in Chapter 3, we will prove Quadratic Reciprocity for the Gaussian Integers. In order to do this, we need to prove extended Quadratic Reciprocity for the integers which allows a negative number in the denominator by following the proof in [7].

Definition 10. For m, n odd integers such that $n > 1$ and $(m, n) = 1$, then $\left(\frac{m}{n}\right) = \left(\frac{m}{-n}\right)$.

This definition makes sense because $-n \equiv n \pmod{n}$, so if m is a quadratic residue with respect to n, then m will be a quadratic residue with respect to $-n$. Before we can state the extended Quadratic Reciprocity Law, we need one more definition.

Definition 11. Let $a \in \mathbb{Z}$, then $\text{sgn } a = \begin{cases} 1 & \text{if } a > 0 \\ -1 & \text{if } a < 0, \end{cases}$ where sgn a is read signum a.

Note: This means $|a| = a \cdot \text{sgn } a$. We now state the following extended theorem of Quadratic Reciprocity which we will prove by following the proof in [12].

Theorem 11. *Let m, n be odd integers such that $(m, n) = 1$ and $m, n \neq -1, 1$, then*

1. $\left(\frac{-1}{n}\right) = (-1)^{[(n-1)/2]+[(sgn\ n-1)/2]}$.

2. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

3. $\left(\frac{m}{n}\right) = (-1)^{[[(m-1)(n-1)]/4]+[[(sgn\ m-1)(sgn\ n-1)]/2]}\left(\frac{n}{m}\right)$.

Proof. To prove the first part of Theorem 11, we must note that for odd integers a and b, $(a-1)(b-1) \equiv 0 \pmod 4$. Since $(a-1)(b-1) = ab - (a+b-1)$, then

$$ab \equiv a + b - 1 \pmod 4$$

$$ab - 1 \equiv (a-1) + (b-1) \pmod 4$$

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2.$$

By Definition 10, $\left(\frac{-1}{n}\right) = \left(\frac{-1}{|n|}\right)$ and by Theorem 10, $\left(\frac{-1}{|n|}\right) = (-1)^{(|n|-1)/2}$. By Definition 11 and the above congruences, we have

$$(-1)^{(|n|-1)/2} = (-1)^{(n\cdot\text{sgn}\ n-1)/2} = (-1)^{[(n-1)/2]+[(\text{sgn}\ p-1)/2]}.$$

This proves part one of Theorem 11.

To prove part two of Theorem 11, we note that $(n)^2 = (-n)^2$ so by part 2 of Theorem 10, part two of Theorem 11 is true.

In order to prove part three of Theorem 11, we first show that

$$\left(\frac{m}{n}\right) = (-1)^{[(\text{sgn}\ m-1)/2][[(n-1)/2]+[(\text{sgn}\ n-1)/2]]}\left(\frac{|m|}{n}\right). \tag{2.9}$$

To see this we consider two cases.

Case 1: Let $m > 0$. By Definition 11, $\left(\frac{m}{n}\right) = \left(\frac{\text{sgn}\ m}{n}\right)\left(\frac{|m|}{n}\right)$ and sgn $m = 1$. This means that $\left(\frac{m}{n}\right) = \left(\frac{|m|}{n}\right)$, which is what happens in the equation (2.9) since

$(-1)^0 = 1$.

Case 2: Let $m < 0$. By Definition 11, $\left(\frac{m}{n}\right) = \left(\frac{\text{sgn } m}{n}\right)\left(\frac{|m|}{n}\right)$ and sgn $m = -1$. This means that $\left(\frac{m}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{|m|}{n}\right)$. By the first part of Theorem 11,

$$\begin{aligned}\left(\frac{-1}{n}\right) &= (-1)^{[(n-1)/2]+[(\text{sgn } n-1)/2]} \\ &= (-1)^{-1[[(n-1)/2]+[(\text{sgn } n-1)/2]]} \\ &= (-1)^{[(\text{sgn } m-1)/2][[(n-1)/2]+[(\text{sgn } n-1)/2]]}\left(\frac{|m|}{n}\right).\end{aligned}$$

This proves equation (2.9).

We make the claim that

$$\left(\frac{|m|}{n}\right) = \left(\frac{n}{m}\right)(-1)^{[(|m|-1)/2][[(|n|-1)/2]+[(\text{sgn } n-1)/2]]}. \tag{2.10}$$

To see this, by Definition 10 and the third part of Theorem 10, we have the following equality:

$$\left(\frac{|m|}{n}\right) = \left(\frac{|m|}{|n|}\right) = \left(\frac{|n|}{|m|}\right)(-1)^{[(|n|-1)(|m|-1)]/2}.$$

Then, by Definition 10 and equation (2.9) we have the following equality:

$$\left(\frac{|n|}{|m|}\right) = \left(\frac{|n|}{m}\right) = \left(\frac{n}{m}\right)(-1)^{[(\text{sgn } n-1)/2][[(m-1)/2]+[(\text{sgn } m-1)/2]]}.$$

By combining these two equations we have the following equation:

$$\left(\frac{|m|}{n}\right) = \left(\frac{n}{m}\right)(-1)^{[(\text{sgn } n-1)/2][[(m-1)/2]+[(\text{sgn } m-1)/2]]}(-1)^{[(|n|-1)(|m|-1)]/2}.$$

By adding the exponents of the (-1)'s and using the fact that for odd integers a and b we have $\frac{ab-1}{2} \equiv (\frac{a-1}{2} + \frac{b-1}{2}) \pmod 2$, we see that

$$\left(\frac{|m|-1}{2}\cdot\frac{|n|-1}{2}\right)+\frac{\text{sgn } n-1}{n}\left(\frac{m-1}{2}+\frac{\text{sgn } m-1}{2}\right) = \frac{|m|-1}{2}\left(\frac{|n|-1}{2}+\frac{\text{sgn } n-1}{n}\right).$$

By combining all three of these equations we get equation (2.10) and the claim holds.

Finally, by combining equations (2.9) and (2.10), we are able to prove the third part of Theorem 11 as follows

$$\begin{aligned}\left(\frac{m}{n}\right) &= (-1)^{[(\text{sgn } m-1)/2][[(n-1)/2]+[(\text{sgn } n-1)/2]]}\left(\frac{|m|}{n}\right)\\ &= (-1)^{[(\text{sgn } m-1)/2][[(n-1)/2]+[(\text{sgn } n-1)/2]]}(-1)^{[(|m|-1)/2][[(|n|-1)/2]+[(\text{sgn } n-1)/2]]}\left(\frac{n}{m}\right).\end{aligned}$$

At this point, we focus on the exponent.

$$\begin{aligned}&[[(\text{sgn } m-1)/2][[(n-1)/2]+[(\text{sgn } n-1)/2]]]\\ &\quad+[[(|m|-1)/2][[(\text{sgn } n-1)/2]+[(|n|-1)/2]]]\\ &=[[(\text{sgn } m-1)/2][(n-1)/2]]+[[(\text{sgn } m-1)/2][(\text{sgn } n-1)/2]]\\ &\quad+[[(|m|-1)/2][(n-1)/2]]\\ &=[[[(\text{sgn } m-1)/2]+[(|m|-1)/2]][(n-1)/2]]+[[(\text{sgn } m-1)/2][(\text{sgn } n-1)/2]]\\ &=[[(m-1)/2][(n-1)/2]]+[[(\text{sgn } m-1)/2][(\text{sgn } n-1)/2]].\end{aligned}$$

This implies that $\left(\frac{m}{n}\right) = (-1)^{[[(m-1)/2][(n-1)/2]]+[[(\text{sgn } m-1)/2][(\text{sgn } n-1)/2]]}\left(\frac{n}{m}\right)$. This proves the final part of Theorem 11. $\square$

Before we move onto Chapter 3, it is interesting to note that both Eisenstein's Lemma and Gauss's Lemma can be generalized even further for the Jacobi Symbol $\left(\frac{m}{n}\right)$ by following the proof in [5]. Since $n \geq 3$ and is an odd, positive integer, we can create $(n-1)/2$ orbits from the nonzero congruence classes modulo n. These two element orbits are as follows $\{1, n-1\}, \{2, n-2\}, ..., \{\frac{n-1}{2}, \frac{n+1}{2}\}$. By multiplying these orbits by m, which is relatively prime to n, then the orbits are permuted among themselves. For example, let $n = 15$ and $m = 7$. For these values the orbits are formed as follows: $\{1, 14\}$, $\{2, 13\}$, $\{3, 12\}$, $\{4, 11\}$, $\{5, 10\}$, $\{6, 9\}$, $\{7, 8\}$. When these orbits are multiplied by 7, the following permutations are formed: $\{1,14\} \to \{7,8\} \to \{4,11\} \to \{2,13\} \to \{1,14\}, \{3,12\} \to \{6,9\} \to \{3,12\}$, and $\{5,10\} \to \{5,10\}$. In looking at Gauss's Lemma, he formed a set R, which took an element from each of the orbits. Gauss chose to take the smallest of the two numbers in each orbit; in the example above, his choice of R was $R = \{1,2,3,4,5,6,7\}$. Once R is established, we want to see how many elements in R permute themselves to an element outside of R. Given that $1 \to 7, 2 \to 14, 3 \to 6, 4 \to 13, 5 \to 5, 6 \to 12$, and $7 \to 4$, then there are three elements of R which permute to an element outside of R. Therefore, by Gauss's choice of R, we have $\left(\frac{7}{15}\right) = (-1)^3 = -1$. In looking at Eisenstein's Lemma, we see that he formed a set R', which took the even element from each orbit, so in the above example $R' = \{2,4,6,8,10,12,14\}$. Given that $2 \to 14, 4 \to 13, 6 \to 12, 8 \to 11, 10 \to 10, 12 \to 9$, and $14 \to 8$, then by Eisenstein's choice of R', $\left(\frac{7}{15}\right) = (-1)^3 = -1$. What would happen if R'' was chosen so that one element was chosen from each orbit at random? For example, let $R'' = \{14,7,11,13,3,9,5\}$. Given that $14 \to 12, 7 \to 4, 11 \to 2, 13 \to 1, 3 \to 6, 9 \to 3$, and $5 \to 5$, then there are 5 elements which are sent outside of R''. While the number 5 is different than the 3 from the first two choices of R, the parity is the same, which means by this choice of R'', $\left(\frac{7}{15}\right) = (-1)^5 = -1$.

Lemma 11. *Let m, n be odd, positive integers such that $n > 1$ and $(m,n) = 1$. The Jacobi Symbol $\left(\frac{m}{n}\right) = (-1)^\mu$ where μ is the number of times an element of R is sent by m to an element outside of R, no matter how the set R is chosen.*

Proof. There are $(n-1)/2$ nonzero congruence classes modulo n of the form $\{x, -x\}$ where $1 \le x \le (n-1)/2$. We need to show that no matter how R is chosen, μ has the same parity. Let $R = \{x, y, z\}$ and assume $x \to -y \to z \to x$ and $-x \to y \to -z \to -x$. If y is replaced with $-y$, then that determines whether x

goes to an element inside or outside of R and it determines whether that second element of R goes to an element inside or outside or R. This means that μ was changed by a factor of two, which means that no matter if μ was even or odd at the beginning, it will remain even or odd with the change of one element. If another element of R is changed, then μ will change by a factor of 2, again leaving μ with the same parity. This continues to the point where it does not matter how R is chosen, as long as each orbit only gives one element to R. $\square$

CHAPTER III
QUADRATIC RECIPROCITY IN THE GAUSSIAN INTEGERS

In Chapter 2, we proved the Law of Quadratic Reciprocity and Gauss's Lemma for the rational integers. In order to show that this law and lemma can also work in the Gaussian integers, we must first discuss the properties of the Gaussian integers. Let $\mathbb{R}$ denote the set of real numbers and $\mathbb{C}$ denote the set of complex numbers. Every complex number can be written uniquely in the form $c + di$, where $c, d \in \mathbb{R}$ and $i^2 = -1$.

Definition 12. The set of *Gaussian integers* is $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

An example of a Gaussian integer would be $6 + 7i$. It is obvious to see that $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$. In order to discuss the Gaussian integers further, we will need to define a few terms.

Definition 13. A *group* $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:

1. For all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.

2. There is an element e in G such that for all $a \in G$, $e * a = a * e = a$.

3. Corresponding to each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = e$.

In the case where $*$ is commutative, the group is said to be abelian.

It is obvious that $\mathbb{Z}[i]$ is an abelian group under addition.

Definition 14. A *ring* $\langle R, +, \cdot \rangle$ is a set R together with the two binary operations $+$ and $\cdot$, which we will call addition and multiplication, defined on R such that the following axioms are satisfied:

1. $\langle R, + \rangle$ is an abelian group.

2. Multiplication is associative.

3. For all $a, b, c \in R$, the left distributive law, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the right distributive law $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

In the case where multiplication is commutative, the ring is called a *commutative ring.* In the case where there exists an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$, the ring is called a *ring with unity* where 1 is the unity.

It is easy to check that $\mathbb{Z}[i]$ is a commutative ring with unity.

Definition 15. If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are *divisors of zero.*

It is simple to verify that $\mathbb{C}$ has no divisors of zero, so obviously $\mathbb{Z}[i]$ has no divisors of zero.

Definition 16. An *integral domain* is a nonzero commutative ring with unity but no divisors of zero.

It is easy to check $\mathbb{Z}[i]$ is an integral domain.

Definition 17. The *norm function* $N : \mathbb{C} \to \mathbb{R}^{+} \cup \{0\}$ is defined by $N(a + bi) = a^2 + b^2$ where $a + bi \in \mathbb{C}$.

For example, $N(3 + 2i) = 9 + 4 = 13$. It is important to note that the norm function is not one to one since $N(2 - 3i) = 13$ and $3 + 2i \neq 2 - 3i$. However, the norm function is multiplicative, that is to say that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{C}$.

Proof. Let $\alpha = a + bi$ and $\beta = c + di$ such that $a, b, c, d \in \mathbb{R}$.

$$N(\alpha\beta) = N[(a + bi)(c + di)] = N[(ac - bd) + (ad + bc)i] = (ac - bd)^2 + (ad + bc)^2$$
$$= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$$
$$= (a^2 + b^2)(c^2 + d^2) = N(a + bi)N(c + di) = N(\alpha)N(\beta).$$

□

Definition 18. An *integral domain* R is said to be a Euclidean domain if there is a function λ from the nonzero elements of R to the set $\{0, 1, 2, 3, ...\}$ such that if $a, b \in R$, $b \neq 0$, there exists $c, d \in R$ with the property $a = cb + d$ and either $d = 0$ or $\lambda(d) < \lambda(b)$.

We claim that $\mathbb{Z}[i]$ is a Euclidean domain with respect to the norm function. We need to show that for $\alpha, \gamma \in \mathbb{Z}[i]$, there exists $\delta, \rho \in \mathbb{Z}[i]$ with the property that $\alpha = \gamma\delta + \rho$ where $\rho = 0$ or $N(\rho) < N(\gamma)$. We follow the proof in [10]. Let $\alpha = a + bi$ and $\gamma = c + di$ where $a, b, c, d \in \mathbb{Z}$. Suppose that $\gamma \neq 0$. This means that $\alpha/\gamma = r + si$ where r and s are rational numbers. Now, choose $m, n \in \mathbb{Z}$ such that $|r - m| \leq 1/2$ and $|s - n| \leq 1/2$. Set $\delta = m + ni$. Then, $\delta \in \mathbb{Z}[i]$ and

$$N[(\alpha/\gamma) - \delta)] = N[(r + si) - (m + ni)] = N[(r - m) + (s - n)i]$$
$$= (r - m)^2 + (s - n)^2 \leq 1/4 + 1/4 = 1/2.$$

Now set $\rho = \alpha - \gamma\delta$. Then, either $\rho = 0$ or $N(\rho) = N(\alpha - \gamma\delta) = N(\gamma((\alpha/\gamma) - \delta)) = N(\gamma)N((\alpha/\gamma) - \delta) \leq 1/2N(\gamma) < N(\gamma)$. Therefore, $\mathbb{Z}[i]$ is an Euclidean domain.

Definition 19. Let a and b be elements of an integral domain R. The element a is said to be a *divisor* of b if there exists $c \in R$ such that $b = ac$. If a is a divisor of b we write $a \mid b$. If a is not a divisor of b we write $a \nmid b$. An element $a \in R$ is called a *unit* if $a \mid 1$. The set of units of R is denoted by $U(R)$.

In $\mathbb{Z}[i]$, $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$. This can be shown by proving that $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$.

Proof. Assume $\alpha \in \mathbb{Z}[i]$ is a unit and γ is the inverse of α. Then, $\alpha\gamma = 1$ and by taking the norm of both sides we have $N(\alpha\gamma) = N(1)$. Since the norm function is multiplicative, then $N(\alpha)N(\gamma) = 1$. Since $N(\alpha)$ and $N(\gamma)$ are both positive integers, then $N(\alpha) = N(\gamma) = 1$.

Now assume $\alpha \in \mathbb{Z}[i]$ such that $\alpha = a + bi$ and $N(\alpha) = 1$. This means that $a^2 + b^2 = 1$. Since $a, b \in \mathbb{Z}$, there are only four possible solutions: $(a, b) = (\pm 1, 0)$ or $(a, b) = (0, \pm 1)$. These four solutions lead to the four units $1, -1, i$, and $-i$. $\square$

Definition 20. Two nonzero elements $a, b \in R$ are said to be *associates* if $a = bu$ where u is a unit in R.

For example, $4 + 3i$ and $-3 + 4i$ are associates since $(4 + 3i)i = 4i - 3$.

Definition 21. Let $\alpha \in \mathbb{Z}[i]$ be given by $\alpha = a + bi$. The *conjugate* of α is $\bar{\alpha} = a - bi$.

For example, if $\alpha = 6 + 7i$, then $\bar{\alpha} = 6 - 7i$.

Definition 22. A nonzero, nonunit element a of an integral domain R is called an *irreducible element*, if $a = bc$, where $b, c \in R$, implies that either b or c is a unit.

Definition 23. A nonzero, nonunit element p of an integral domain R is called a *prime* if $p \mid ab$, where $a, b \in R$, implies that $p \mid a$ or $p \mid b$.

Definition 24. An *ideal* I of an integral domain R is a nonempty subset of R having the following two properties:

1. $a, b \in I$ implies $a - b \in I$,

2. $a \in I, r \in R$ implies $ra \in I$.

Definition 25. An ideal I of an integral domain R is called a *principal ideal* if there exists a fixed $a \in I$ such that $I = \langle a \rangle = \{ra \mid r \in R\}$. The element a is called a generator of the ideal I. An ideal I of an integral domain R is called a *proper ideal* if $I \neq 0$ or R. A proper ideal I of an integral domain R is called a *prime ideal* if $a, b \in R$ and $ab \in I$ implies $a \in I$ or $b \in I$.

Definition 26. An integral domain R is said to be a *principal ideal domain (PID)* if every ideal of R is principal.

Since every Euclidean domain is a PID, this means that $\mathbb{Z}[i]$ is a PID [11]. Also, in a PID, every irreducible element is a prime element, so every irreducible element of $\mathbb{Z}[i]$ is prime [11]. There are three different types of primes in $\mathbb{Z}[i]$. In order to see this, we first must prove a lemma and a theorem.

Lemma 12. *If $\alpha \in \mathbb{Z}[i]$, and $N(\alpha)$ is a prime in $\mathbb{Z}$, then α is prime in $\mathbb{Z}[i]$.*

Proof. Following the proof in [10], assume $\alpha = \mu\lambda$ with $\mu, \lambda \in \mathbb{Z}[i]$. Then, $N(\alpha) = N(\mu\lambda) = N(\mu)N(\lambda)$. Since $N(\alpha)$ is a prime by assumption, then either $N(\mu) = 1$ or $N(\lambda) = 1$, so either μ or λ is a unit in $\mathbb{Z}[i]$. By Definition 22, this means that α is irreducible in $\mathbb{Z}[i]$ which means that α is a prime in $\mathbb{Z}[i]$. $\square$

Recall Theorem 4 in Chapter 1, which stated that for p an odd prime in $\mathbb{Z}$, there exists $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ if and only if $p \equiv 1 \pmod 4$. We are now able to prove Theorem 4.

Proof. First, we show that if p is a rational prime such that $p \equiv 3 \pmod 4$, then p cannot be written as the sum of two squares. In working modulo 4, if an integer x is an even integer, then $x^2 \equiv 0 \pmod 4$. If $a \equiv 1 \pmod 2$, then $a^2 \equiv 1 \pmod 4$. This means that $a^2 + b^2$ can not be congruent to $3 \pmod 4$. Therefore, $p \equiv 3 \pmod 4$ cannot be written as the sum of two squares.

Now, assume p is an odd prime such that $p \equiv 1 \pmod 4$. By part 1 of Theorem 7, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Since $p \equiv 1 \pmod 4$, this means that

$$\left(\frac{-1}{p}\right) = (-1)^{(4k+1-1)/2} = (-1)^{4k/2} = 1$$

for some $k \in \mathbb{Z}$. By Definition 7, this means there exists $b \in \mathbb{Z}$ such that $b^2 \equiv -1 \pmod p$, so $p \mid b^2 + 1$. By factoring $b^2 + 1$ in $\mathbb{Z}[i]$, this means that $p \mid (b+i)(b-i)$. Since $p > 1$, $p \nmid (b+i)$ and $p \nmid (b-i)$. This implies that p is not a prime in $\mathbb{Z}[i]$ and is therefore a reducible element in $\mathbb{Z}[i]$. Therefore, $p = \alpha\beta$, with $\alpha, \beta \in \mathbb{Z}[i]$ both nonunits. By taking the norm of both sides, we are left with the equation

$$N(p) = p^2 = N(\alpha)N(\beta).$$

Since $N(\alpha)$ and $N(\beta)$ are both > 1, then $p = N(\alpha)$ and $p = N(\beta)$. Since $\alpha \in \mathbb{Z}[i]$, then $\alpha = a + bi$ for $a, b \in \mathbb{Z}$. Therefore $p = a^2 + b^2$, so p can be written as the sum of two squares. □

Now that we have Lemma 12 and Theorem 4, we will be able to prove that there are three different types of primes in $\mathbb{Z}[i]$ which we will call Gaussian primes following the proofs in [10]. First, $1 + i$ is a Gaussian prime. This is easy to see since $N(1+i) = 2$. Since 2 is a prime in $\mathbb{Z}$, by Lemma 12, $1+i$ is a Gaussian prime. It is important to note that $2 = (1+i)(i-1)$ and $1+i$ and $1-i$ are associates since $1+i = i(1-i)$. This means that in terms of Gaussian primes, $1+i$ and $1-i$ are the "same" and so $1+i$ is the only "even" Gaussian prime.

The next type of Gaussian prime is any prime $p \in \mathbb{Z}$ such that $p \equiv 3 \pmod 4$. Assume by way of contradiction that p was not a Gaussian prime. This would mean that p was not an irreducible element of $\mathbb{Z}[i]$, which implies that there exists $\alpha, \beta \in \mathbb{Z}[i]$ with $p = \alpha\beta$ and $N(\alpha) > 1$ and $N(\beta) > 1$ by Definition 22. By taking the norm of both sides of the equation, we have $N(p) = N(\alpha\beta)$ which implies $p^2 = N(\alpha)N(\beta)$. Therefore, $p = N(\alpha)$. Let $\alpha = a + bi$ where $a, b \in \mathbb{Z}$. This means that $p = a^2 + b^2$ which contradicts Theorem 4 since $p \equiv 3 \pmod 4$. Therefore, p is a Gaussian prime. In fact, p is considered to be an odd Gaussian prime.

For the final type of Gaussian prime, let p be a prime in $\mathbb{Z}$ such that $p \equiv 1 \pmod 4$. By Theorem 4, this means that $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$, which means $p = \pi\bar{\pi}$ with $\pi = a+bi$ and $\bar{\pi} = a-bi$. Since $N(\pi) = p$ and $N(\bar{\pi}) = p$, by Lemma 12, both π and $\bar{\pi}$ are Gaussian primes. We claim that π and $\bar{\pi}$ are not associates, and so π and $\bar{\pi}$ are actually distinct Gaussian primes. Assume by way of contradiction that $\pi, \bar{\pi} \in \mathbb{Z}[i]$ are associates. By Definition 20, there exists a unit $u \in \mathbb{Z}[i]$ such that $u\pi = \bar{\pi}$ which implies $u(a + bi) = a - bi$.

Case 1: Assume that $1(a + bi) = a - bi$. This means that $b = -b$ which means $2b = 0$. Therefore, $p = a^2$ which implies $a \mid p$. Since p is a rational prime, by Definition 1, $a = \pm 1$ or $a = \pm p$. If $a = \pm 1$, then $p = 1$ which is a contradiction since p is a rational prime. If $a = \pm p$, then

$$\begin{aligned} p &= p^2 \\ p - p^2 &= 0 \\ p(1-p) &= 0 \\ p &= 0 \quad \text{or} \quad p = 1 \end{aligned}$$

which is also a contradiction since p is a rational prime.

Case 2: Assume that $-1(a + bi) = a - bi$. This means that $a = -a$ which means $2a = 0$. Therefore, $p = b^2$ which implies $b \mid p$. By a similar argument as in

Case 1, we find a contradiction.

Case 3: Assume that $i(a+bi) = a - bi$. This means that $-b + ai = a - bi$ which means $a = -b$. Therefore, $p = 2a^2$ which implies that $2 \mid p$. This is a contradiction since p is odd.

Case 4: Assume that $-i(a+bi) = a-bi$. This means that $b-ai = a-bi$ which means $a = b$. Therefore, $p = 2a^2$ which again leads to a contradiction. Therefore, π and $\bar{\pi}$ are not associates, so they are distinct Gaussian primes. It should be noted that π and $\bar{\pi}$ are both odd Gaussian primes.

There is one last important property of the Gaussian integers that needs to be proved, but first we need another definition and lemma.

Definition 27. A *field* is a commutative ring R with unity $1 \neq 0$ such that every element of R has a multiplicative inverse in R. A subring Q of a field R is a *subfield* of R if Q is itself a field.

Lemma 13. *Let F be a finite field. The integer multiples of the multiplicative identity, namely, 1_F, $2 \cdot 1_F = 1_F + 1_F$, $3 \cdot 1_F = 1_F + 1_F + 1_F$, et cetera, form a subfield of F isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Proof. We refer to [10] for a proof. □

Theorem 12. *If π is an irreducible element in $\mathbb{Z}[i]$, then the residue class ring $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a finite field with $N(\pi)$ elements.*

Proof. We know that $\mathbb{Z}[i]$ is a PID. Let $\alpha \in \mathbb{Z}[i]$ be such that α is not congruent to $0 \pmod{\pi}$. There exists $\beta, \gamma \in \mathbb{Z}[i]$ such that $\beta\alpha + \gamma\pi = 1$ since α and π are relatively prime [5]. Then, $\gamma\pi = 1 - \beta\alpha$ which implies $\beta\alpha \equiv 1 \pmod{\pi}$. This means that the residue class of α is a unit in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. Therefore, $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a field by Lemma 13 [10].

Next, we need to show $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ has $N(\pi)$ elements. We know π is irreducible, so π is a prime. We will need to look at three different cases.

Case 1: Suppose $\pi = 1 + i$. Let $\alpha \in \mathbb{Z}[i]$, then since $\mathbb{Z}[i]$ is a Euclidean Domain, there exists $\gamma, \rho \in \mathbb{Z}[i]$ such that $\alpha = \delta(1 + i) + \rho$ where either $\rho = 0$ or $N(\rho) < N(i+1)$, so $N(\rho) < 2$ which means $\rho \in \{0, 1, -1, i, -i\}$. However, we claim that every element in $\mathbb{Z}[i]$ is congruent to either 0 or 1 modulo $(1+i)$. Let $\alpha = a+bi$ be in $\mathbb{Z}[i]$. If $(1 + i) \mid \alpha$, then $\alpha \equiv 0 \pmod{1 + i}$, and we are done.

If $1 + i$ does not divide α, then $\frac{a+bi}{1+i} = \frac{a+bi}{1+i}\frac{1-i}{1-i} = [(a + b) + (b - a)i]/2$. Since $1 + i$ does not divide $a + bi$, then one of $a + b$ or $b - a$ must be odd, but if $a + b$ is odd, then $b-a$ is odd. This means that both $[(a - 1) + b]$ and $[b - (a - 1)]$ are even. Therefore $(1 + i) \mid (a + bi) - 1$, which implies $a + bi \equiv 1 \pmod{1 + i}$. Thus every element in $\mathbb{Z}[i]$ is congruent to either 0 or 1 modulo $(1 + i)$ and 0 is not congruent to 1 modulo $(1 + i)$, so a complete set of coset representatives is $\{0, 1\} \pmod{\pi}$. Since every element in $\mathbb{Z}[i]$ falls into one of two cosets modulo $1+i$, that means the number of elements in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is $2 = N(\pi) = N(1 + i)$.

Case 2: Suppose $\pi = q \equiv 3 \pmod 4$ where q is a rational prime. We claim that $\{a + bi \mid 0 \le a, b \le q - 1\}$ is a complete set of coset representatives modulo π. This will show that $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ has $N(q) = q^2$ elements. Let $\mu = m + ni \in \mathbb{Z}[i]$. If $m = qs + a$ and $n = qt + b$, where $s, t, a, b \in \mathbb{Z}$ and $0 \le a, b \le q - 1$, then $\mu \equiv a + bi \pmod{q}$.

Now suppose that $a + bi \equiv a' + b'i \pmod{q}$ where $0 \le a, b, a', b' \le q - 1$. This means that $\frac{a-a'}{q} + \left(\frac{b-b'}{q}\right)i \in \mathbb{Z}[i]$, so $\frac{a-a'}{q}, \frac{b-b'}{q} \in \mathbb{Z}$. The only way those elements could be integers is if $a = a'$ and $b = b'$ since $0 \le a, b, a', b' < q$. Therefore, $\{a + bi \mid 0 \le a, b \le q - 1\}$ is a complete set of coset representatives modulo q. Since every element in $\mathbb{Z}[i]$ is congruent to exactly one element in $\{a+bi \mid 0 \le a, b \le q-1\} \pmod{q}$, there are $q^2 = N(q)$ elements in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ since there are q possibilities for a and q possibilities for b. Please note that $q^2 \equiv 1 \pmod 4$.

Case 3: Now suppose that $p \equiv 1 \pmod 4$ is a rational prime and $\pi\bar{\pi} = N(\pi) = p$. We claim that $\{0, 1, 2, ..., p-1\}$ is a complete set of coset representatives modulo π. This will show that $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ has $p = N(\pi)$ elements. Let $\pi = a + bi$ where $a, b \in \mathbb{Z}$. Then $p = a^2 + b^2$ with $0 < b < p$, so $p \nmid b$. Now let $\mu = m + ni$ where $m, n \in \mathbb{Z}$. Since $p \nmid b$, then $(p, b) = 1$ since p is a prime. Therefore, there exists $l, k \in \mathbb{Z}$ such that $-pl + bk = 1$ which means

$$-pln + bkn = n$$

$$pln = bkn - n$$

$$p \mid bkn - n.$$

This implies that there exists $c \in \mathbb{Z}$ such that $cb \equiv n \pmod p$. Now $\mu - c\pi = \mu - ca - cbi$ and $\mu - ca - cbi \equiv \mu - ca - ni \equiv m + ni - ca - ni \equiv m - ca \pmod p$. Therefore, $\mu - c\pi \equiv m - ca \pmod{\pi\bar{\pi}}$ which means $\mu \equiv m - ca \pmod \pi$. Since $m, c, a \in \mathbb{Z}$, then $\mu \in \mathbb{Z}[i]$ is congruent to a rational integer modulo π and $\mu \in \mathbb{Z}[i]$ was chosen arbitrarily.

Now, we want to show every rational integer is congruent modulo π to an element in $\{0, 1, 2, ..., p-1\}$. If $l \in \mathbb{Z}$, then $l = sp + r$ where $s, r \in \mathbb{Z}$ and $0 \leq r < p$. This means that

$$l \equiv r \pmod p$$

$$l \equiv r \pmod{\pi\bar{\pi}}$$

$$\pi\bar{\pi} \mid l - r$$

$$\pi \mid l - r$$

$$l \equiv r \pmod \pi.$$

Since each element of $\mathbb{Z}[i]$ is congruent to a rational integer, and every rational integer is congruent to an element in $\{0, 1, 2, ..., p-1\} \pmod \pi$, then every element of $\mathbb{Z}[i]$ is congruent to an element in $\{0, 1, 2, ..., p-1\} \pmod{\pi}$. If $r \equiv r' \pmod{\pi}$ with $r, r' \in \mathbb{Z}$ and $0 \leq r, r' < p$, then $r - r' = \pi\gamma$ and $(r - r')^2 = pN(\gamma)$. Therefore, $p \mid r - r'$ which implies $r = r'$ since $0 \leq r, r' < p$. Therefore, $\{0, 1, 2, ..., p-1\}$ is a complete set of coset representatives modulo π. Since every element in $\mathbb{Z}[i]$ is congruent to exactly one element in $\{0, 1, 2, ..., p-1\} \pmod{\pi}$, there are $p = N(\pi)$ elements in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ since there are p elements in $\{0, 1, 2, ..., p-1\}$. □

Now that we know some properties of the Gaussian integers, we will now show that the Law of Quadratic Reciprocity holds also in the Gaussian integers by following the proof in [9].

Definition 28. Let $k, m \in \mathbb{Z}[i]$ with $N(m) > 1$ and $(k, m) = 1$. The Gaussian integer k is said to be a *quadratic residue of* m if $x^2 \equiv k \pmod{m}$ has a solution $x \in \mathbb{Z}[i]$. The Gaussian integer k is said to be a *quadratic nonresidue of* m if no such solution exists in $\mathbb{Z}[i]$.

This definition is analogous to Definition 6 which defines quadratic residues and nonresidues for the rational integers.

Definition 29. Let $k, m \in \mathbb{Z}[i]$ be such that m is an odd Gaussian prime and $m \nmid k$. The *Gaussian Legendre symbol* $\left[\frac{k}{m}\right]$ is defined as follows:

$$\left[\frac{k}{m}\right] = \begin{cases} 1 & \text{if} \quad x^2 \equiv k \pmod{m} \quad \text{has a solution } x \in \mathbb{Z}[i]. \\ -1 & \text{if} \quad \text{there is no such solution.} \end{cases}$$

It is important to note that the Legendre symbol and the Gaussian Legendre symbol are not always the same. For example, let $k = 2$ and $m = 3$. The Legendre symbol $\left(\frac{2}{3}\right) = -1$, while the Gaussian Legendre symbol $\left[\frac{2}{3}\right] = 1$. This is true since $i^2 = -1 \equiv 2 \pmod{3}$ and $(2i)^2 = -4 \equiv 2 \pmod{3}$. Recall that Dirichlet proved

Theorem 8 for the rational primes. He also proved an analogous theorem for the Gaussian primes as follows:

Theorem 13. *Let $k, m \in \mathbb{Z}[i]$ be such that m is an odd Gaussian prime and $m \nmid k$. If $p = N(m)$, then $k^{(p-1)/2} \equiv \left[\frac{k}{m}\right] \pmod{m}$.*

Proof. Let $k, m \in \mathbb{Z}[i]$ be such that m is an odd Gaussian prime and $m \nmid k$. The nonzero congruence classes modulo $\langle m \rangle$ form a multiplicative group with $s = N(m) - 1$ elements. Let $M = \{\mu_1, \mu_2, ..., \mu_s\}$, where M is a complete system of nonzero residues modulo m. We claim that for each $\mu \in M$ there is a unique $x \in M$ such that $\mu x \equiv k \pmod{m}$. Since $m \nmid k$, then k is congruent modulo m to exactly one element $\alpha \in M$. Given $\mu_j \in M$ for $1 \leq j \leq s$, there exists a unique element $z \in M$ such that $\mu_j z \equiv 1 \pmod{m}$. By multiplying through by α, we are left with the congruence

$$\mu_j(z\alpha) \equiv \alpha \equiv k \pmod{m}.$$

Therefore, $x \equiv z\alpha \pmod{m}$ for $x \in M$.

Case 1: Assume that k is a quadratic nonresidue of m. By Definition 28, this means that $x \neq \mu$. Therefore, M can be partitioned into distinct pairs such that the product of the elements in a pair is congruent to $k \pmod{m}$. Since m is an odd Gaussian prime, by Theorem 12 there are $(p-1)/2$ such pairs where $p = N(m)$. Therefore, by multiplication we have $\mu_1\mu_2 \cdots \mu_s \equiv k^{(p-1)/2} \pmod{m}$.

Case 2: Assume k is a quadratic residue of m. By Definition 28, this means there exists $\mu \in M$ such that $\mu^2 \equiv k \pmod{m}$. If $\mu \in M$ is a solution to $x^2 \equiv k \pmod{m}$, then $-\mu$ will also be a solution since $(-\mu)^2 = \mu^2 \equiv k \pmod{m}$. Assume that $\mu' \in M$ is such that $-\mu \equiv \mu' \pmod{m}$. Note that $\mu \neq \mu'$ since m is an odd Gaussian prime. By removing these two elements from M, the remaining elements can be partitioned into $(p-3)/2$ distinct pairs as in Case 1. The product of these $s-2$

elements in M is congruent to $k^{(p-3)/2}$ modulo m. We also have $\mu\mu' \equiv -k \pmod{m}$. By multiplying these two congruences together, we have $\mu_1\mu_2\cdots\mu_s \equiv -k^{(p-1)/2} \pmod{m}$. As the product $\mu_1\mu_2\cdots\mu_s$ is independent of the Gaussian integer k, we are able to determine it by attributing to k any particular value. If $k = 1$, we have $\mu_1\mu_2\cdots\mu_s \equiv -1 \pmod{m}$. Note that this is the analogue to Wilson's Theorem (Theorem 9) in the rational integers. This results in the congruence $k^{(p-1)/2} \equiv 1 \pmod{m}$ when k is a quadratic residue of m and $k^{(p-1)/2} \equiv -1 \pmod{m}$ when k is a quadratic nonresidue of m. Therefore, by Definition 29, $k^{(p-1)/2} \equiv \left[\frac{k}{m}\right] \pmod{m}$. $\square$

As in the rational integers, there are properties of $\left[\frac{k}{m}\right]$ which can be very useful when working with the Gaussian Legendre symbol.

Theorem 14. *Let $k, l, m \in \mathbb{Z}[i]$ where m is an odd Gaussian prime and m does not divide k or l.*

1. *If $k \equiv l \pmod{m}$, then $\left[\frac{k}{m}\right] = \left[\frac{l}{m}\right]$.*

2. $\left[\frac{k}{m}\right]\left[\frac{l}{m}\right] = \left[\frac{kl}{m}\right]$.

Proof. For the first part of Theorem 14, let $k, l, m \in \mathbb{Z}[i]$ be such that m is an odd Gaussian prime and $k \equiv l \pmod{m}$. If $x^2 \equiv k \pmod{m}$ has a solution in $\mathbb{Z}[i]$, then $x^2 \equiv l \pmod{m}$ has a solution in $\mathbb{Z}[i]$. If $x^2 \equiv k \pmod{m}$ doesn't have a solution in $\mathbb{Z}[i]$, then $x^2 \equiv l \pmod{m}$ also doesn't have a solution in $\mathbb{Z}[i]$. Therefore, $\left[\frac{k}{m}\right] = \left[\frac{l}{m}\right]$.

For the second part of Theorem 14, by Theorem 13, we have the following congruence:

$$\left[\frac{k}{m}\right]\left[\frac{l}{m}\right] \equiv k^{(p-1)/2} l^{(p-1)/2} \equiv (kl)^{(p-1)/2} \equiv \left[\frac{kl}{m}\right] \pmod{m}$$

where $p = N(m)$. Since m is an odd Gaussian prime, $m \nmid 2$, so $\left[\frac{k}{m}\right]\left[\frac{l}{m}\right] = \left[\frac{kl}{m}\right]$. $\square$

Now, we want to show that every Gaussian Legendre symbol $\left[\frac{k}{m}\right]$ can be expressed in terms of a Legendre symbol in the rational integers. Before we can show this, note that $\left[\frac{k}{m}\right]$ does not change if m is replaced by one of its associates. Let $m, k \in \mathbb{Z}[i]$ where m is an odd Gaussian prime and $m \nmid k$. Consider the congruence $x^2 \equiv k \pmod{m}$ which implies $m \mid x^2 - k$. If $m \mid x^2 - k$, then $um \mid x^2 - k$, where u is a unit in $\mathbb{Z}[i]$, which means $x^2 \equiv k \pmod{um}$. Therefore, $\left[\frac{k}{m}\right]$ does not change if m is replaced by one of its associates.

If $m = a + bi$ is an odd Gaussian prime, then $N(m) = a^2 + b^2$ is odd, so a has to be even and b has to be odd or a has to be odd and b has to be even. Since we know that $\left[\frac{k}{m}\right]$ doesn't change if m is replaced by one of its associates, from here on we will assume that a is an odd, positive, rational integer and b is an even rational integer.

For the first case, we will assume that $b = 0$, so $m = a$ where a is an odd positive rational prime such that $a \equiv 3 \pmod{4}$. Let $k = \alpha + \beta i$ where $\alpha, \beta \in \mathbb{Z}$. In order to know the value of $\left[\frac{k}{m}\right] = \left[\frac{\alpha+\beta i}{a}\right]$, we must find if

$$x^2 \equiv (\alpha + \beta i) \pmod{a} \tag{3.1}$$

has a solution in $\mathbb{Z}[i]$. Let $x = \phi + \psi i$ with $\phi, \psi \in \mathbb{Z}$. This means that $[(\phi^2 - \psi^2) + 2\phi\psi i] \equiv (\alpha + \beta i) \pmod{a}$, which can be decomposed into the following two congruences involving only rational integers:

$$(\phi^2 - \psi^2) \equiv \alpha, \; 2\phi\psi \equiv \beta \pmod{a}. \tag{3.2}$$

By squaring each congruence in equation (3.2) and adding them together, the result is:

$$(\phi^4 - 2\phi^2\psi^2 + \psi^4 + 4\phi^2\psi^2) = (\phi^2 + \psi^2)^2 \equiv (\alpha^2 + \beta^2) \pmod{a}.$$

We always assume that $m \nmid k$, so $a \nmid (\alpha + \beta i)$. Suppose for a contradiction that $a \mid (\alpha^2 + \beta^2)$. Since a is prime, by Definition 23, $a \mid (\alpha + \beta i)$ or $a \mid (\alpha - \beta i)$. Since $a \nmid (\alpha + \beta i)$, then $a \nmid \alpha$ or $a \nmid \beta$. This means that $a \nmid (\alpha - \beta i)$ which is a contradiction. Since $a \nmid (\alpha^2 + \beta^2)$, then by Definition 7

$$\left(\frac{\alpha^2 + \beta^2}{a}\right) = 1. \tag{3.3}$$

This means that if there is a solution for congruence (3.1), then equation (3.3) holds true. We claim that if equation (3.3) holds, then congruence (3.1) is solvable which means the congruences in (3.2) have simultaneous solutions.

Case 1: Assume $\alpha \equiv 0 \pmod{a}$. If $\alpha \equiv 0 \pmod{a}$, then equation (3.3) clearly holds since $\left(\frac{\beta^2}{a}\right) = 1$. If we set $\psi = \pm\phi$, then the first congruence in (3.2) holds true. The second congruence will then become $2\phi^2 \equiv \pm\beta \pmod{a}$. We know there exists $f \in \mathbb{Z}$ such that $2f \equiv 1 \pmod{a}$ since $a \nmid 2$. Now, assume that $\left(\frac{f\beta}{a}\right) = 1$. This means there exists $y \in \mathbb{Z}$ such that $y^2 \equiv f\beta \pmod{a}$ which means $2y^2 \equiv \beta \pmod{a}$. This means we can set $\phi = \psi = y$. Now, assume $\left(\frac{f\beta}{a}\right) = -1$. Since $\left(\frac{-f\beta}{a}\right) = \left(\frac{-1}{a}\right)\left(\frac{f\beta}{a}\right) = 1$ by part 1 of Theorem 7, there exists $y \in \mathbb{Z}$ such that $y^2 \equiv -f\beta \pmod{a}$ which means $2y^2 \equiv -\beta \pmod{a}$. This means we can set $\phi = -\psi = y$ and both congruences in congruence (3.2) have a simultaneous solution. Therefore, congruence (3.1) is solvable.

Case 2: Assume $a \nmid \alpha$. Since we are assuming that equation (3.3) holds, then, by Definition 7, there exists $s \in \mathbb{Z}$ such that $s^2 \equiv (\alpha^2 + \beta^2) \pmod{a}$. This means $s^2 - \beta^2 = (s-\beta)(s+\beta) \equiv \alpha^2 \pmod{a}$. Since $\left(\frac{\alpha^2}{a}\right) = 1$, we see that $1 = \left(\frac{s^2-\beta^2}{a}\right) = \left(\frac{s-\beta}{a}\right)\left(\frac{s+\beta}{a}\right)$ or that $\left(\frac{s-\beta}{a}\right) = \left(\frac{s+\beta}{a}\right)$. We now wish to show that s can be chosen so that $\left(\frac{s-\beta}{a}\right) = \left(\frac{s+\beta}{a}\right) = 1$. Since the original congruence was $s^2 \equiv \alpha^2 + \beta^2 \pmod{a}$, we may replace s with $-s$. If $\left(\frac{s-\beta}{a}\right) = \left(\frac{s+\beta}{a}\right) = -1$, then we can replace s with $-s$ producing the equality

$$\left(\frac{-s-\beta}{a}\right) = \left(\frac{-s+\beta}{a}\right) = -1$$
$$\left(\frac{-1}{a}\right)\left(\frac{s+\beta}{a}\right) = \left(\frac{-1}{a}\right)\left(\frac{s-\beta}{a}\right) = -1.$$

Since $a \equiv 3 \pmod{4}$, by part 1 of Theorem 7

$$-\left(\frac{s+\beta}{a}\right) = -\left(\frac{s-\beta}{a}\right) = -1$$
$$\text{or} \quad \left(\frac{s+\beta}{a}\right) = \left(\frac{s-\beta}{a}\right) = 1.$$

Therefore, if s is chosen appropriately, both Legendre symbols will equal 1. Then, by Definition 7, there exists $t, u \in \mathbb{Z}$ with $t^2 \equiv s + \beta \pmod{a}$ and $u^2 \equiv s - \beta \pmod{a}$.

As a result, $(tu)^2 \equiv s^2 - \beta^2 \equiv \alpha^2 \pmod{a}$ which implies $tu \equiv \pm\alpha \pmod{a}$ where the $+$ and $-$ are dependent on the choices of t and u. It is important to note that t and u can be chosen as even or odd at will: If t is odd, then $t_1 = a - t$ is even since a is odd and furthermore $t_1^2 \equiv s + \beta \pmod{a}$, which shows we may replace t by t_1. Therefore, let us assume that t and u are both even. Let $\phi = (t \pm u)/2$ and $\psi = (t \mp u)/2$ (note that both ϕ and ψ are rational integers) where the signs are chosen to conform to the sign in the congruence $tu \equiv \pm\alpha \pmod{a}$. We will check that $\phi = (t+u)/2$ and $\psi = (t-u)/2$ satisfy the congruences in (3.2) when $tu \equiv \alpha \pmod{a}$. From (3.2), we wish to verify that $\phi^2 - \psi^2 \equiv \alpha \pmod{a}$. By making the proper substitutions, we have

$$\begin{aligned}[(t+u)/2]^2 - [(t-u)/2]^2 &= [(t^2+2ut+u^2)/4] - [(t^2-2ut+u^2)/4] \\ &= (ut/2) + (ut/2) = ut\end{aligned}$$

and we know $ut \equiv \alpha \pmod{a}$, so the first congruence holds true. We want to show the second congruence in (3.2), $2\phi\psi \equiv \beta \pmod{a}$ or $4\phi\psi \equiv 2\beta \pmod{a}$, also holds true when $\phi = (t+u)/2$ and $\psi = (t-u)/2$. By making the proper substitutions, we have

$$\begin{aligned}4[(t+u)/2][(t-u)/2] &\equiv (t+u)(t-u) \equiv t^2 - u^2 \\ &\equiv s + \beta - s + \beta \equiv 2\beta \pmod{a}.\end{aligned}$$

Therefore, the congruences in (3.2) have simultaneous solutions. It is easy to check that $\phi = (t-u)/2$ and $\psi = (t+u)/2$ satisfy the congruences in (3.2) when $tu \equiv -\alpha \pmod{a}$. Therefore, the congruence in (3.1) has a solution in $\mathbb{Z}[i]$ when (3.3) holds.

This means that $\left[\frac{\alpha+\beta i}{a}\right] = 1$ if and only if $\left(\frac{\alpha^2+\beta^2}{a}\right) = 1$. Since both of these symbols only have the values of 1 or -1, this implies that

$$\left[\frac{\alpha+\beta i}{a}\right] = \left(\frac{\alpha^2+\beta^2}{a}\right). \tag{3.4}$$

For the second case, we will assume that $m = a + bi$ where $a, b \in \mathbb{Z}\backslash\{0\}$ and m is an odd Gaussian prime which divides a rational prime $p = N(m) = a^2 + b^2 \equiv 1 \pmod{4}$. Recall that we are assuming a is an odd, positive, rational integer and b is an even integer. We will let $k = \alpha + \beta i$ where $\alpha, \beta \in \mathbb{Z}$ and $m \nmid k$. We wish to determine if the congruence $x^2 \equiv \alpha + \beta i \pmod{m}$ has a solution $x \in \mathbb{Z}[i]$. Our first claim is that $(a, b) = 1$. Assume by way of contradiction that $(a, b) = d$ where $d \in \mathbb{Z}$ is greater than 1. This means $d \mid a$ and $d \mid b$ by Definition 3. Therefore, there exists $c + ei \in \mathbb{Z}[i]$ such that $a + bi = d(c + ei)$. Therefore, $N(a + bi) = N(d)N(c + ei)$, so $p = d^2(c^2 + e^2)$ which is a contradiction since $p = N(m)$ is prime. Therefore, $(a, b) = 1$.

From the proof of Theorem 12, we know $\{0, 1, ..., p-1\}$ is a complete set of congruence class representatives modulo m. Therefore, we can limit ourselves to $x \in \mathbb{Z}$ when deciding whether $x^2 \equiv \alpha + \beta i \pmod{m}$ has a solution or not. The congruence $x^2 \equiv \alpha + \beta i \pmod{m}$ is solvable if and only if there exist $x, \phi, \psi \in \mathbb{Z}$ such that $x^2 - \alpha - \beta i = (\phi + \psi i)(a + bi)$. This leads to the following two equations consisting entirely of rational integers:

$$x^2 - \alpha = a\phi - b\psi \quad \text{and} \quad -\beta = b\phi + a\psi. \tag{3.5}$$

By multiplying the first equation by a and the second equation by b, and then adding them together, the result is:

$$ax^2 - a\alpha - b\beta = a^2\phi - ab\psi + b^2\phi + ab\psi = (a^2 + b^2)\phi = p\phi. \tag{3.6}$$

We now claim that $p \nmid a\alpha + b\beta$.

Proof. Since $p = a^2 + b^2$, then $1 \leq a, |b| < p$ and so $p \nmid a$ and $p \nmid b$. Since $m \nmid k = \alpha + \beta i$, we have $\alpha + \beta i \equiv y \pmod{m}$ with $1 \leq y \leq p-1$ which implies $p \nmid y$. This congruence means that $y - \alpha - \beta i = (u + vi)(a + bi)$ where $u, v \in \mathbb{Z}$. By the same process as in equations (3.5) and (3.6), $ay - a\alpha - b\beta = up$ which implies $p \mid ay - a\alpha - b\beta$. If $p \mid a\alpha + b\beta$, then $p \mid ay$ which is a contradiction by Definition 23, since $p \nmid a$ and $p \nmid y$. Therefore, $p \nmid a\alpha + b\beta$. Note that this is true whether the congruence $x^2 \equiv y \pmod{m}$ has a solution or not. □

If the congruence $x^2 \equiv \alpha + \beta i \pmod{m}$ has a solution $x \in \mathbb{Z}$ then equation (3.6) implies that $ax^2 \equiv a\alpha + b\beta \pmod{p}$. Since $p \nmid a\alpha + b\beta$ this implies by parts 2 and 3 of Theorem 6 that

$$\left(\frac{ax^2}{p}\right) = \left(\frac{a}{p}\right) = \left(\frac{a\alpha + b\beta}{p}\right). \tag{3.7}$$

We now wish to show conversely that if equation (3.7) holds, then the congruence $x^2 \equiv \alpha + \beta i \pmod{m}$ has a solution $x \in \mathbb{Z}$. First, we show that equation (3.7) implies equation (3.6).

Proof. Assume that $\left(\frac{a}{p}\right) = \left(\frac{a\alpha+b\beta}{p}\right)$. Since $p \nmid a$ and $p \nmid a\alpha + b\beta$, there exists a unique z with $1 \leq z \leq p-1$ such that $az \equiv a\alpha + b\beta \pmod{p}$. Therefore, by parts 2 and 3 of Theorem 6, $\left(\frac{a\alpha+b\beta}{p}\right) = \left(\frac{az}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{z}{p}\right)$. By assumption, this means that $\left(\frac{z}{p}\right) = 1$. Therefore, there exists $x \in \mathbb{Z}$ with $1 \leq x \leq p-1$ such that $x^2 \equiv z \pmod{p}$. As a result, $ax^2 \equiv a\alpha + b\beta \pmod{p}$ which means $ax^2 - a\alpha - b\beta = p\phi$ for some $\phi \in \mathbb{Z}$. Therefore, equation (3.7) implies equation (3.6). $\square$

Since $p = a^2 + b^2$, the equation $ax^2 - a\alpha - b\beta = p\phi$ leads to the following sequence of equations:

$$\begin{aligned} ax^2 - a\alpha - b\beta &= (a^2+b^2)\phi \\ ax^2 - a\alpha - b\beta &= a^2\phi + b^2\phi \\ ax^2 - a\alpha - a^2\phi &= b^2\phi + b\beta \\ a(x^2 - \alpha - a\phi) &= b(\beta + b\phi). \end{aligned}$$

This equation implies that $a \mid b(\beta + b\phi)$ which implies $a \mid (\beta + b\phi)$ since $(a, b) = 1$. Therefore, $-a\psi = \beta + b\phi$ for some $\psi \in \mathbb{Z}$. This means that $a(x^2 - \alpha - a\phi) = b(-a\psi)$ which means that $x^2 - \alpha - a\phi = -b\psi$. From this it follows that equation (3.7) implies both equations in (3.5) hold and therefore that the congruence $x^2 \equiv \alpha + \beta i \pmod{m}$ has a solution $x \in \mathbb{Z}$. Equation (3.7) may be rewritten as $\left(\frac{a}{p}\right)\left(\frac{a\alpha+b\beta}{p}\right) = 1$ and we have just shown that if this equation holds then $\left[\frac{\alpha+\beta i}{a+bi}\right] = 1$. By our previous work we conclude that $\left[\frac{\alpha+\beta i}{a+bi}\right] = 1$ if and only if $\left(\frac{a}{p}\right)\left(\frac{a\alpha+b\beta}{p}\right) = 1$. From this and the fact that the left hand sides only take on the possible values of 1 or -1 we conclude that we always have an equality of values $\left[\frac{\alpha+\beta i}{a+bi}\right] = \left(\frac{a}{p}\right)\left(\frac{a\alpha+b\beta}{p}\right)$. We may simplify this last equality one step further by now proving that $\left(\frac{a}{p}\right) = 1$. Recall that a is odd and positive. If $a = 1$, then clearly $\left(\frac{a}{p}\right) = 1$. If $a > 1$, we may employ quadratic reciprocity for Jacobi symbols (part 3 of Theorem 10) to deduce that $\left(\frac{a}{p}\right) = (-1)^{[(a-1)(p-1)]/4}\left(\frac{p}{a}\right)$. Since $p \equiv 1 \pmod 4$, this simply becomes $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)$. Since $p = a^2 + b^2$, we have $p \equiv b^2 \pmod a$ and therefore $\left(\frac{p}{a}\right) = \left(\frac{b^2}{a}\right)$ by part 2 of Proposition 1 in Chapter II. By part 1 of Proposition 1 we have $\left(\frac{b^2}{a}\right) = \left(\frac{b}{a}\right)\left(\frac{b}{a}\right)$ and the right hand side is equal to 1 since $\left(\frac{b}{a}\right)$ is either 1 or -1. We conclude that $\left(\frac{a}{p}\right) = 1$ and so

$$\left[\frac{\alpha+\beta i}{a+bi}\right] = \left(\frac{a\alpha+b\beta}{p}\right). \tag{3.8}$$

Equations (3.4) and (3.8), taken together, show that every Gaussian Legendre symbol can be expressed in terms of a Legendre symbol in the rational integers. These crucial equations were originally proved by Dirichlet [9] and they will allow us to reduce the proof of quadratic reciprocity for the Gaussian integers back to quadratic reciprocity for the rational integers.

Now, to prove that the Law of Quadratic Reciprocity can be applied to the Gaussian integers, we need another definition.

Definition 30. Let R be an integral domain. Then R is said to be a *factorization domain* if every nonzero, nonunit element of R can be expressed as a finite product of irreducible elements of R. If every nonzero, nonunit element of R has a unique factorization as a product of irreducible elements of R, then R is called a *unique factorization domain (UFD).*

Since $\mathbb{Z}[i]$ is a PID, this means that $\mathbb{Z}[i]$ is a UFD [11]. Let m be a fixed odd Gaussian prime. Let $k \in \mathbb{Z}[i]$ be such that $(k, m) = 1$. Since $\mathbb{Z}[i]$ is a UFD, then $k = (\pm 1)(i)^{0 \text{ or } 1}(1+i)^t(l_1)^{s_1} \cdots (l_n)^{s_n}$ where the l_i are distinct odd Gaussian primes, t is a nonnegative integer, and the s_i are nonnegative integers with $1 \leq i \leq n$. By Theorem 14, this means that

$$\left[\frac{k}{m}\right] = \left[\frac{\pm 1}{m}\right]\left[\frac{i}{m}\right]^{0 \text{ or } 1}\left[\frac{1+i}{m}\right]^t\left[\frac{l_1}{m}\right]^{s_1} \cdots \left[\frac{l_n}{m}\right]^{s_n}.$$

It is obvious that $\left[\frac{\pm 1}{m}\right] = 1$. This leads to the corresponding Law of Quadratic Reciprocity for the Gaussian integers where parts 1, 2, and 3 correspond to parts 1, 2, and 3 of Theorem 7.

Theorem 15. *Let $a + bi, \alpha + \beta i \in \mathbb{Z}[i]$ be distinct odd Gaussian primes such that $a, \alpha \in \mathbb{Z}^+$ are odd and $b, \beta \in \mathbb{Z}$ are even or 0. Let $p = a^2 + b^2$ and note that p is not a prime if $b = 0$ whereas p is a prime if $b \neq 0$. Either way, $p > 1$, $p \equiv 1 \pmod 4$, and the following three properties hold for the Gaussian Legendre symbol.*

1. $\left[\frac{i}{a+bi}\right] = (-1)^{(p-1)/4}$.

2. $\left[\frac{1+i}{a+bi}\right] = (-1)^{((a+b)^2-1)/8}$.

3. $\left[\frac{\alpha+\beta i}{a+bi}\right] = \left[\frac{a+bi}{\alpha+\beta i}\right]$.

Proof. For part 1 of Theorem 15, we know by Theorem 13 that $(i)^{(p-1)/2} \equiv \left[\frac{i}{a+bi}\right] \pmod{a+bi}$. Note that $(i)^{(p-1)/2} = (i^2)^{(p-1)/4}$, so $(-1)^{(p-1)/4} \equiv \left[\frac{i}{a+bi}\right] \pmod{a+bi}$. Since both sides of this last congruence are either 1 or -1, if they are not equal then $-1 \equiv 1 \pmod{a+bi}$ which implies $-2 = (a+bi)(c+di)$ where $c, d \in \mathbb{Z}$. Therefore,

$N(-2) = N(a+bi)N(c+di)$, so $p \mid 4$ which is a contradiction since $p \equiv 1 \pmod 4$ and $p > 1$. Therefore, $\left[\frac{i}{a+bi}\right] = (-1)^{(p-1)/4}$.

For part 2 of Theorem 15, we look at two different cases.

Case 1: Let $b = 0$, so $p = a^2$ where $a \in \mathbb{Z}^+$ is a prime with $a \equiv 3 \pmod 4$. By equation (3.4), $\left[\frac{1+i}{a}\right] = \left(\frac{1+1}{a}\right) = \left(\frac{2}{a}\right)$. By part 2 of Theorem 7, $\left(\frac{2}{a}\right) = (-1)^{(a^2-1)/8}$.

Case 2: Let $b \neq 0$. By equation (3.8), $\left[\frac{1+i}{a+bi}\right] = \left(\frac{a+b}{p}\right)$. Note that $a+b$ is odd, it is relatively prime to p and it is possibly negative as well. If $|a+b| = 1$, then $\left(\frac{a+b}{p}\right) = 1$ (recall that p is a rational prime in this case congruent to 1 modulo 4 and so $\left(\frac{-1}{p}\right) = 1$ by part 1 of Theorem 7). The expression on the right side of part 2 of Theorem 15 is also equal to 1 when $|a+b| = 1$. We assume from now on that $|a+b| > 1$ and we may use part 3 of Theorem 11 to see that

$$\left(\frac{a+b}{p}\right) = (-1)^{[[(p-1)/2][(a+b-1)/2]]+[[(\text{sgn } p-1)(\text{sgn } (a+b)-1)]/2]}\left(\frac{p}{a+b}\right).$$

Since $p \equiv 1 \pmod 4$, then $(p-1)/2$ is even, so $[(p-1)/2][(a+b-1)/2]$ is even. Since p is positive, then $[(\text{sgn } p - 1)(\text{sgn } (a+b) - 1)]/2 = 0$. This implies that $\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right)$. By Definition 10, $\left(\frac{p}{a+b}\right) = \left(\frac{p}{|a+b|}\right)$ and we have proved thus far that $\left[\frac{1+i}{a+bi}\right]$ is equal to the Jacobi symbol $\left(\frac{p}{|a+b|}\right)$. In order to complete the proof of part 2 we first note that

$$2p = 2a^2 + 2b^2 = a^2 + 2ab + b^2 + a^2 - 2ab + b^2 = (a+b)^2 + (a-b)^2.$$

Since $a+b$ divides the quantity $(a-b)^2 - (a+b)^2 - (a-b)^2 = (a-b)^2 - 2p$, there exists a solution to the congruence $x^2 \equiv 2p \pmod{|a+b|}$. By part 1 of Proposition 1 we have

$$\left(\frac{x^2}{|a+b|}\right) = \left(\frac{x}{|a+b|}\right)\left(\frac{x}{|a+b|}\right) = 1.$$

By part 2 of Proposition 1, we have

$$\left(\frac{2p}{|a+b|}\right) = \left(\frac{x^2}{|a+b|}\right) = 1.$$

By part 1 of Proposition 1, we have

$$\left(\frac{2}{|a+b|}\right)\left(\frac{p}{|a+b|}\right) = 1$$

or that $\left(\frac{2}{|a+b|}\right) = \left(\frac{p}{|a+b|}\right)$. By what was shown above and by part 2 of Theorem 10 we have

$$\left(\frac{p}{|a+b|}\right) = \left(\frac{2}{|a+b|}\right) = (-1)^{((|a+b|)^2-1)/8} = (-1)^{((a+b)^2-1)/8},$$

and so $\left[\frac{1+i}{a}\right] = (-1)^{((a+b)^2-1)/8}$.

For part 3 of Theorem 15, we look at three different cases.

Case 1: Let $b = \beta = 0$. By equation (3.4), $\left[\frac{\alpha}{a}\right] = \left(\frac{\alpha^2}{a}\right) = 1$. Likewise, $\left[\frac{a}{\alpha}\right] = \left(\frac{a^2}{\alpha}\right) = 1$. Therefore, $\left[\frac{\alpha}{a}\right] = \left[\frac{a}{\alpha}\right]$.

Case 2: Assume $\beta = 0$ and $b \neq 0$. By equation (3.8), $\left[\frac{\alpha}{a+bi}\right] = \left(\frac{a\alpha}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{\alpha}{p}\right) = \left(\frac{\alpha}{p}\right)$ (in the proof of (3.8) it was shown that $\left(\frac{a}{p}\right) = 1$). By equation (3.4), $\left[\frac{a+bi}{\alpha}\right] = \left(\frac{a^2+b^2}{\alpha}\right) = \left(\frac{p}{\alpha}\right)$. By part 3 of Theorem 7, we know that $\left(\frac{\alpha}{p}\right) = (-1)^{[(p-1)(\alpha-1)]/4}\left(\frac{p}{\alpha}\right)$. Since $p \equiv 1 \pmod 4$ this equality reduces to $\left(\frac{\alpha}{p}\right) = \left(\frac{p}{\alpha}\right)$, and therefore $\left[\frac{\alpha}{a+bi}\right] = \left[\frac{a+bi}{\alpha}\right]$.

Case 3: Assume neither β or b equals 0. Since both $a + bi$ and $\alpha + \beta i$ are distinct odd Gaussian primes, by equation (3.8), $\left[\frac{\alpha+\beta i}{a+bi}\right] = \left(\frac{a\alpha+b\beta}{p}\right)$ and $\left[\frac{a+bi}{\alpha+\beta i}\right] = \left(\frac{a\alpha+b\beta}{w}\right)$ where $p = a^2+b^2$ and $w = \alpha^2+\beta^2$. Note that $a\alpha+b\beta$ is odd, relatively prime to p, and it is possibly negative. If $|a\alpha + b\beta| = 1$, then $\left(\frac{a\alpha+b\beta}{p}\right) = \left(\frac{a\alpha+b\beta}{w}\right) = 1$ by part 1 of Theorem 7 since both p and w are rational primes congruent to 1 modulo 4 in this case. Since we have shown that the third part of Theorem 15 is true when $|a\alpha + b\beta| = 1$, we will assume from now on that $|a\alpha + b\beta| > 1$. We note that

$$\begin{aligned}(a\alpha + b\beta)^2 + (b\alpha - a\beta)^2 &= a^2\alpha^2 + 2ab\alpha\beta + b^2\beta^2 + b^2\alpha^2 - 2ab\alpha\beta + a^2\beta^2 \\ &= a^2\alpha^2 + a^2\beta^2 + b^2\alpha^2 + b^2\beta^2 \\ &= (a^2 + b^2)(\alpha^2 + \beta^2) = pw.\end{aligned}$$

Since $a\alpha + b\beta$ divides $(b\alpha - a\beta)^2 - (a\alpha + b\beta)^2 - (b\alpha - a\beta)^2 = (b\alpha - a\beta)^2 - pw$, there exists a solution to the congruence $x^2 \equiv pw \pmod{|a\alpha + b\beta|}$. By Definition 10, we have $\left(\frac{x^2}{a\alpha+b\beta}\right) = \left(\frac{x^2}{|a\alpha+b\beta|}\right)$. By part 1 of Proposition 1, we have

$$\left(\frac{x^2}{|a\alpha + b\beta|}\right) = \left(\frac{x}{|a\alpha + b\beta|}\right)\left(\frac{x}{|a\alpha + b\beta|}\right) = 1.$$

By part 2 of Proposition 1, we have

$$\left(\frac{pw}{|a\alpha + b\beta|}\right) = \left(\frac{x^2}{|a\alpha + b\beta|}\right) = 1.$$

By part 1 of Proposition 1, we have

$$\left(\frac{pw}{|a\alpha + b\beta|}\right) = \left(\frac{p}{|a\alpha + b\beta|}\right)\left(\frac{w}{|a\alpha + b\beta|}\right) = 1.$$

This implies that $\left(\frac{p}{|a\alpha+b\beta|}\right) = \left(\frac{w}{|a\alpha+b\beta|}\right)$, and by Definition 10 this means that $\left(\frac{p}{a\alpha+b\beta}\right) = \left(\frac{w}{a\alpha+b\beta}\right)$. Since $|a\alpha + b\beta| > 1$, part 3 of Theorem 11 leads to $\left(\frac{a\alpha+b\beta}{p}\right) = \left(\frac{a\alpha+b\beta}{w}\right)$ since $p, w \equiv 1 \pmod 4$ and both $p, w > 0$. Therefore, by equation (3.8), $\left[\frac{\alpha+\beta i}{a+bi}\right] = \left[\frac{a+bi}{\alpha+\beta i}\right]$. $\square$

Now that we have proven Theorem 15, we would like to extend this theorem to odd Gaussian integers $M = A + Bi$ where M is not necessarily prime.

Definition 31. An odd Gaussian integer is an element $M \in \mathbb{Z}[i]$ which is not a unit in $\mathbb{Z}[i]$ and which is only divisible by odd Gaussian primes. Let $M = m_1 m_2 \cdots m_n$, where each m_i is an odd Gaussian prime (we do not assume they are necessarily distinct among themselves). Let k be a Gaussian integer which is not divisible by m_i for $1 \le i \le n$. The *Gaussian Jacobi symbol* $\left[\frac{k}{M}\right]$ is defined in terms of Gaussian Legendre symbols as $\left[\frac{k}{M}\right] = \left[\frac{k}{m_1}\right]\left[\frac{k}{m_2}\right]\cdots\left[\frac{k}{m_n}\right]$.

It is important to note that like the Jacobi symbol, the Gaussian Jacobi symbol cannot determine if k is a quadratic residue of M, but only if k is a quadratic nonresidue of M. Like the Gaussian Legendre symbol, the Gaussian Jacobi symbol has some important properties.

Theorem 16. *Let M and M' be odd Gaussian integers and assume that each is relatively prime to both $k, l \in \mathbb{Z}[i]$.*

1. *If $k \equiv l \pmod{M}$, then $\left[\frac{k}{M}\right] = \left[\frac{l}{M}\right]$.*

2. $\left[\frac{k}{M}\right]\left[\frac{l}{M}\right] = \left[\frac{kl}{M}\right]$.

3. $\left[\frac{k}{MM'}\right] = \left[\frac{k}{M}\right]\left[\frac{k}{M'}\right]$.

Proof. For the first part, we write $M = m_1 m_2 \cdots m_n$ as in Definition 31. Using part 1 of Theorem 14, we obtain

$$\left[\frac{k}{M}\right] = \left[\frac{k}{m_1}\right]\left[\frac{k}{m_2}\right]\cdots\left[\frac{k}{m_n}\right] = \left[\frac{l}{m_1}\right]\left[\frac{l}{m_2}\right]\cdots\left[\frac{l}{m_n}\right] = \left[\frac{l}{M}\right].$$

For the second part, we use Definition 31 and part 2 of Theorem 14 to show that

$$\begin{aligned}
\left[\frac{k}{M}\right]\left[\frac{l}{M}\right] &= \left[\frac{k}{m_1}\right]\left[\frac{k}{m_2}\right]\cdots\left[\frac{k}{m_n}\right]\left[\frac{l}{m_1}\right]\left[\frac{l}{m_2}\right]\cdots\left[\frac{l}{m_n}\right] \\
&= \left[\frac{k}{m_1}\right]\left[\frac{l}{m_1}\right]\left[\frac{k}{m_2}\right]\left[\frac{l}{m_2}\right]\cdots\left[\frac{k}{m_n}\right]\left[\frac{l}{m_n}\right] \\
&= \left[\frac{kl}{m_1}\right]\left[\frac{kl}{m_2}\right]\cdots\left[\frac{kl}{m_n}\right] \\
&= \left[\frac{kl}{M}\right].
\end{aligned}$$

For the third part, we write $M' = m_1'm_2'\cdots m_t'$ as in Definition 31 to obtain

$$\begin{aligned}
\left[\frac{k}{MM'}\right] &= \left[\frac{k}{m_1}\right]\left[\frac{k}{m_2}\right]\cdots\left[\frac{k}{m_n}\right]\left[\frac{k}{m_1'}\right]\left[\frac{k}{m_2'}\right]\cdots\left[\frac{k}{m_t'}\right] \\
&= \left[\frac{k}{M}\right]\left[\frac{k}{M'}\right].
\end{aligned}$$

□

We now wish to show that Theorem 15 has a direct generalization to the Gaussian Jacobi symbol in the same way that we were able to generalize from Theorem 7 to Theorem 10 for the usual Legendre and Jacobi symbols.

Theorem 17. *Let $A + Bi$ and $\alpha + \beta i$ be odd Gaussian integers which are relatively prime to each other and such that $A, \alpha \in \mathbb{Z}$ are odd and $B, \beta \in \mathbb{Z}$ are even or zero. Let $P = A^2 + B^2$ and note that $P \equiv 1 \pmod 4$. The following three properties hold for the Gaussian Jacobi symbol.*

1. $\left[\frac{i}{A+Bi}\right] = (-1)^{(P-1)/4}$.

2. $\left[\frac{1+i}{A+Bi}\right] = (-1)^{((A+B)^2-1)/8}$.

3. $\left[\frac{\alpha+\beta i}{A+Bi}\right] = \left[\frac{A+Bi}{\alpha+\beta i}\right]$.

Proof. We do a proof by induction to show the first part of this theorem holds true.
Base case: By Theorem 15, we know that $\left[\frac{i}{a+bi}\right] = (-1)^{(p-1)/4}$ where $a+bi$ is an odd Gaussian prime and $p = a^2+b^2$.
Induction Hypothesis: Assume that $\left[\frac{i}{A+Bi}\right] = (-1)^{(P-1)/4}$ where $A+Bi$ is an odd Gaussian integer and $P = A^2+B^2$. We want to show that $\left[\frac{i}{A'+B'i}\right] = (-1)^{(P'-1)/4}$, where $A'+B'i = (A+Bi)(a+bi)$ is an odd Gaussian integer divisible by one more Gaussian prime than $A+Bi$ and $P' = A'^2+B'^2$. By part 3 of Theorem 16,

$$\left[\frac{i}{A'+B'i}\right] = \left[\frac{i}{A+Bi}\right]\left[\frac{i}{a+bi}\right] = (-1)^{(P-1)/4}(-1)^{(p-1)/4} = (-1)^{[(P-1)/4]+[(p-1)/4]}.$$

We need to show that $(p-1)/4+(P-1)/4$ and $(P'-1)/4$ have the same parity in order to complete the induction step. We note that

$$\begin{aligned}(pP-1)/4-(p-1)/4-(P-1)/4 &= pP/4-p/4-P/4+1/4\\ &= (pP-p-P+1)/4\\ &= (p(P-1)-(P-1))/4\\ &= ((p-1)(P-1))/4.\end{aligned}$$

Also, note that since $N(A'+B'i) = N(A+Bi)N(a+bi)$, then $P' = Pp$. Since both $P, p \equiv 1 \pmod 4$, the quantity $((p-1)(P-1))/4$ is even (it is actually divisible by 4). This means that the left hand side of the equation is also even, so $(p-1)/4+(P-1)/4$ and $(P'-1)/4$ have the same parity. Therefore, $\left[\frac{i}{A'+B'i}\right] = (-1)^{(P'-1)/4}$, which completes the inductive step.

We also do a proof by induction to show the second part of the theorem.
Base case: By Theorem 15, we know that $\left[\frac{1+i}{a+bi}\right] = (-1)^{(r^2-1)/8}$ where $a+bi$ is an

odd Gaussian prime and $r = a + b$.

Induction Hypothesis: Assume that $\left[\frac{1+i}{A+Bi}\right] = (-1)^{(s^2-1)/8}$ where $A + Bi$ is an odd Gaussian integer and $s = A + B$. We want to show that $\left[\frac{1+i}{A'+B'i}\right] = (-1)^{(t^2-1)/8}$, where $A' + B'i = (A + Bi)(a + bi)$ is an odd Gaussian integer divisible by one more Gaussian prime than $A + Bi$ and $t = A' + B'$. By part 3 of Theorem 16,

$$\left[\frac{1+i}{A'+B'i}\right] = \left[\frac{1+i}{A+Bi}\right]\left[\frac{1+i}{a+bi}\right] = (-1)^{(s^2-1)/8}(-1)^{(r^2-1)/8} = (-1)^{[(s^2-1)/8]+[(r^2-1)/8]}.$$

We need to show that $(r^2 - 1)/8 + (s^2 - 1)/8$ and $(t^2 - 1)/8$ have the same parity in order to complete the induction step. We note that

$$\begin{aligned}
((rs)^2 - 1)/8 - (r^2 - 1)/8 - (s^2 - 1)/8 &= (rs)^2/8 - r^2/8 - s^2/8 + 1/8 \\
&= (r^2s^2 - r^2 - s^2 + 1)/8 \\
&= (r^2(s^2 - 1) - (s^2 - 1))/8 \\
&= ((r^2 - 1)(s^2 - 1))/8.
\end{aligned}$$

Since r and s are odd integers, $r^2, s^2 \equiv 1 \pmod 8$, which means that the quantity $((r^2 - 1)(s^2 - 1))/8$ is even. Further, this means that $[((a + b)(A + B))^2 - 1]/8 = ((rs)^2-1)/8$ and $[(r^2-1)/8]+[(s^2-1)/8]$ have the same parity. Let $z = (a+b)(A+B)$ and note that z is odd. Since b and B are both even, $2bB$ is divisible by 8, so let $8q = 2bB$ for some $q \in \mathbb{Z}$. We claim that $[((a + b)(A + B))^2 - 1]/8$ and $[((a + b)(A + B) - 2bB)^2 - 1]/8$ have the same parity. To verify this, note that

$$\begin{aligned}
&[((a + b)(A + B) - 2bB)^2 - 1]/8 \\
&= [(z - 8q)^2 - 1]/8 = [z^2 - 16zq + 64q^2 - 1]/8 \\
&= [((a + b)(A + B))^2 - 1]/8 + [-16qz + 64q^2]/8
\end{aligned}$$

and since $[-16qz + 64q^2]/8$ is even we see that the two quantities of interest have the same parity as claimed. We have proved thus far that $\left[\frac{1+i}{A'+B'i}\right] = (-1)^v$, where

$v = [((a+b)(A+B)-2bB)^2-1]/8$. We now prove that $((a+b)(A+B)-2bB)^2 = t^2$, which will finally complete the induction step. Since $A' = aA - bB$ and $B' = aB + bA$, we have

$$
\begin{aligned}
&((a+b)(A+B)-2bB)^2 \\
&= (a+b)^2(A+B)^2 - 4(a+b)(A+B)(bB) + 4b^2B^2 \\
&= (a^2+2ab+b^2)(A^2+2AB+B^2) - 4[aA+aB+bA+bB](bB) + 4b^2B^2 \\
&= a^2A^2 + 2a^2AB + a^2B^2 + 2abA^2 + 4abAB + 2abB^2 + b^2A^2 + 2b^2AB + b^2B^2 \\
&\ - 4abAB - 4abB^2 - 4b^2AB \\
&= a^2A^2 + 2a^2AB + a^2B^2 + 2abA^2 - 2abB^2 + b^2A^2 - 2b^2AB + b^2B^2 \\
&= a^2A^2 + b^2B^2 + 2a^2AB + 2abA^2 - 2abB^2 - 2b^2AB + a^2B^2 + b^2A^2 \\
&= (aA-bB)^2 + 2(aA-bB)(aB+bA) + (aB+bA)^2 \\
&= [(aA-bB)+(aB+bA)]^2 = (A'+B')^2 = t^2.
\end{aligned}
$$

For the third part of Theorem 17, recall that both $\alpha+\beta i$ and $A+Bi$ are odd Gaussian integers. By Definition 31, this means that $\alpha+\beta i = \pi_1\pi_2\cdots\pi_m$, where each π_i is an odd Gaussian prime and $A+Bi = \lambda_1\lambda_2\cdots\lambda_n$, where each λ_j is an odd Gaussian prime. Therefore, by Definition 31, we have

$$\left[\frac{\alpha+\beta i}{A+Bi}\right] = \left[\frac{\pi_1\pi_2\cdots\pi_m}{\lambda_1\lambda_2\cdots\lambda_n}\right] = \left[\frac{\pi_1\pi_2\cdots\pi_m}{\lambda_1}\right]\cdots\left[\frac{\pi_1\pi_2\cdots\pi_m}{\lambda_n}\right].$$

By part 2 of Theorem 14, we have

$$\left[\frac{\pi_1\pi_2\cdots\pi_m}{\lambda_1}\right]\cdots\left[\frac{\pi_1\pi_2\cdots\pi_m}{\lambda_n}\right] = \left[\frac{\pi_1}{\lambda_1}\right]\cdots\left[\frac{\pi_m}{\lambda_1}\right]\cdots\left[\frac{\pi_1}{\lambda_n}\right]\cdots\left[\frac{\pi_m}{\lambda_n}\right].$$

By part 3 of Theorem 15, we have

$$
\begin{aligned}
\left[\frac{\pi_1}{\lambda_1}\right]\cdots\left[\frac{\pi_m}{\lambda_1}\right]\cdots\left[\frac{\pi_1}{\lambda_n}\right]\cdots\left[\frac{\pi_m}{\lambda_n}\right] &= \left[\frac{\lambda_1}{\pi_1}\right]\cdots\left[\frac{\lambda_1}{\pi_m}\right]\cdots\left[\frac{\lambda_n}{\pi_1}\right]\cdots\left[\frac{\lambda_n}{\pi_m}\right] \\
&= \left[\frac{\lambda_1}{\pi_1}\right]\cdots\left[\frac{\lambda_n}{\pi_1}\right]\cdots\left[\frac{\lambda_1}{\pi_m}\right]\cdots\left[\frac{\lambda_n}{\pi_m}\right].
\end{aligned}
$$

By part 2 Theorem 14, we have

$$\left[\frac{\lambda_1}{\pi_1}\right] \cdots \left[\frac{\lambda_n}{\pi_1}\right] \cdots \left[\frac{\lambda_1}{\pi_m}\right] \cdots \left[\frac{\lambda_n}{\pi_m}\right] = \left[\frac{\lambda_1 \lambda_2 \cdots \lambda_n}{\pi_1}\right] \cdots \left[\frac{\lambda_1 \lambda_2 \cdots \lambda_n}{\pi_m}\right].$$

Finally, by Definition 31 we have

$$\left[\frac{\lambda_1 \lambda_2 \cdots \lambda_n}{\pi_1}\right] \cdots \left[\frac{\lambda_1 \lambda_2 \cdots \lambda_n}{\pi_m}\right] = \left[\frac{\lambda_1 \lambda_2 \cdots \lambda_n}{\pi_1 \pi_2 \cdots \pi_m}\right] = \left[\frac{A + Bi}{\alpha + \beta i}\right].$$

□

We will conclude this thesis by constructing Gauss's Lemma in the Gaussian integers by following the argument in [5]. Let S be the analogous set (to be defined later) to the set R from Lemma 11.

Lemma 14 (Gauss's Lemma). *Let $\kappa, \beta \in \mathbb{Z}[i]$ be such that $(\kappa, \beta) = 1$ and β is odd. Then $\left[\frac{\kappa}{\beta}\right] = (-1)^{\mu}$, where μ is the number of times an element of S is sent outside of S via multiplication by κ.*

First, recall Theorem 12 which stated that the residue class ring $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a finite field with $N(\pi)$ elements when π is an irreducible element in $\mathbb{Z}[i]$. In order to construct Gauss's Lemma, we need the following proposition:

Proposition 2. *If β is a nonzero element of $\mathbb{Z}[i]$, then the quotient ring $\mathbb{Z}[i]/\langle\beta\rangle$ has $N(\beta)$ elements.*

Proof. First note that if β is a unit in $\mathbb{Z}[i]$, then $\mathbb{Z}[i] = \langle\beta\rangle$ and $N(\beta) = 1$ so that the proposition holds trivially in this case. From now on we assume β is not a unit and we first handle the case where β is a Gaussian prime power. Let $\pi \in \mathbb{Z}[i]$ be a fixed Gaussian prime. Let M be a complete set of congruence class representatives modulo $\langle\pi\rangle$. By Theorem 12, we know that M has $N(\pi)$ elements. We first want to show that given $n \in \mathbb{Z}^+$, $T = \{c_0 + c_1\pi + \cdots + c_{n-1}\pi^{n-1} \mid c_0, c_1, ..., c_{n-1} \in M\}$ is a complete set of congruence class representatives modulo $\langle \pi^n \rangle$.

We need to show that every element in $\mathbb{Z}[i]$ is congruent to a unique element of T modulo $\langle \pi^n \rangle$. Let $\alpha \in \mathbb{Z}[i]$ be such that $\alpha = a + bi$, where $a, b \in \mathbb{Z}$. We first describe an algorithm for constructing an element of T that is congruent to α modulo $\langle \pi^n \rangle$. We will give a concrete example of how this algorithm works in practice below. As a first step, there exists a unique element $c_0 \in M$ such that $\alpha \equiv c_0 \pmod{\pi}$. We may write $\alpha = \gamma_1\pi + c_0$ for some $\gamma_1 \in \mathbb{Z}[i]$. If $\gamma_1 = 0$ we are done, if not there exists a unique $c_1 \in M$ such that $\gamma_1 \equiv c_1 \pmod{\pi}$. We may write $\gamma_1 = \gamma_2\pi + c_1$ for some $\gamma_2 \in \mathbb{Z}[i]$. If $\gamma_2 = 0$, then we are done, if not there exists a unique $c_2 \in M$ such that $\gamma_2 \equiv c_2 \pmod{\pi}$. We may write $\gamma_2 = \gamma_3\pi + c_2$ for some $\gamma_3 \in \mathbb{Z}[i]$. This algorithm continues for a finite number of steps until there exists a unique element element $c_{n-1} \in M$ such that $\gamma_{n-1} \equiv c_{n-1} \pmod{\pi}$. We may write $\gamma_{n-1} = \gamma_n\pi + c_{n-1}$ for some $\gamma_n \in \mathbb{Z}[i]$. We use the equations we just constructed and substitution to see that

$$\begin{aligned}
\alpha &= \gamma_1\pi + c_0 \\
&= (\gamma_2\pi + c_1)\pi + c_0 = \gamma_2\pi^2 + c_1\pi + c_0 \\
&= (\gamma_3\pi + c_2)\pi^2 + c_1\pi + c_0 = \gamma_3\pi^3 + c_2\pi^2 + c_1\pi + c_0 \\
&= ... = \gamma_n\pi^n + c_{n-1}\pi^{n-1} + \cdots + c_2\pi^2 + c_1\pi + c_0.
\end{aligned}$$

This means that $\alpha \equiv (c_0 + c_1\pi + c_2\pi^2 + \cdots + c_{n-1}\pi^{n-1}) \pmod{\pi^n}$. For an example of this algorithm, let $\pi = 1 + 2i$, $n = 3$, and $\alpha = 6 + 5i$. By Theorem 12 (see the proof of case 3), we know that $M = \{0, 1, 2, 3, 4\}$. We can easily check that $6 + 5i \equiv 1 \pmod{1 + 2i}$, so we can write the equation $6 + 5i = (3 - i)(1 + 2i) + 1$. Now we look at $3 - i$ and realize that $3 - i \equiv 1 \pmod{1 + 2i}$, so we can write the equation $3 - i = (-i)(1 + 2i) + 1$. Now we look at $-i$ and realize that $-i \equiv 3 \pmod{1 + 2i}$, so we can write the equation $-i = (-1 + i)(1 + 2i) + 3$. Since $n = 3$ for this example, we can stop at this equation. We now use substitution to see that

$$\begin{aligned}6+5i &= (3-i)(\pi)+1\\ &= [(-i)(\pi)+1](\pi)+1 = (-i)(\pi)^2+\pi+1\\ &= [(-1+i)(\pi)+3](\pi)^2+\pi+1 = (-1+i)(\pi)^3+3\pi^2+\pi+1.\end{aligned}$$

This means that $6+5i \equiv 1+1\cdot\pi+3\cdot\pi^2 \pmod{\pi^3}$.

Now, we need to show that every element in T is distinct modulo π^n. Assume that two elements of T are congruent modulo π^n, say

$$a_0+a_1\pi+\cdots+a_{n-1}\pi^{n-1} \equiv b_0+b_1\pi+\cdots+b_{n-1}\pi^{n-1} \pmod{\pi^n},$$

where $a_i, b_i \in M$ for $0 \le i \le n-1$. This means there exists $\gamma \in \mathbb{Z}[i]$ such that

$$(a_0-b_0)+(a_1-b_1)\pi+\cdots+(a_{n-1}-b_{n-1})\pi^{n-1} = \gamma\pi^n.$$

This means that

$$a_0-b_0 = \pi[\gamma\pi^{n-1}-((a_1-b_1)+\cdots+(a_{n-1}-b_{n-1})\pi^{n-2})].$$

This implies that $a_0 \equiv b_0 \pmod{\pi}$ and so $a_0 = b_0$ since $a_0, b_0 \in M$. This process can be repeated to show that $a_1 = b_1, \ldots, a_{n-1} = b_{n-1}$. This means that the elements in T are all distinct from each other modulo π^n and thus T is a complete set of congruence class representatives modulo $\langle\pi^n\rangle$. Since M has $N(\pi)$ elements, the number of elements in T is $[N(\pi)]^n = N(\pi^n)$.

Since $\mathbb{Z}[i]$ is a PID, we may now apply the Chinese Remainder Theorem to handle the case where β is divisible by more than one Gaussian prime. Let β_1, β_2 be nonzero nonunits in $\mathbb{Z}[i]$ that are relatively prime to one another. Let T_1 and T_2 be complete sets of congruence representatives modulo $\langle\beta_1\rangle$ and $\langle\beta_2\rangle$, respectively. Given any ordered pair $(t_i, t_j) \in T_1 \times T_2$, the Chinese Remainder Theorem states that there exists an element $\gamma_{ij} \in \mathbb{Z}[i]$ such that $\gamma_{ij} \equiv t_i \pmod{\langle\beta_1\rangle}$ and $\gamma_{ij} \equiv t_j$

(mod $\langle\beta_2\rangle$), and if γ'_{ij} is another simultaneous solution to these two congruences, then $\gamma_{ij} \equiv \gamma'_{ij} \pmod{\langle\beta_1\beta_2\rangle}$.

We can use the Chinese Remainder Theorem to run through all the pairs $(t_i, t_j) \in T_1 \times T_2$ to find a simultaneous solution γ_{ij} for the congruences above for each (t_i, t_j). These γ_{ij}'s will form a complete set of congruence class representatives modulo $\langle\beta_1\beta_2\rangle$. If $\beta_1 = \pi_1^{n_1}$ and $\beta_2 = \pi_2^{n_2}$ for $n_1, n_2 \in \mathbb{Z}^+$, where π_1 and π_2 are distinct Gaussian primes, then T_1 has $N(\pi_1^{n_1})$ elements and T_2 has $N(\pi_2^{n_2})$ elements and so $T_1 \times T_2$ has $N(\pi_1^{n_1}) \cdot N(\pi_2^{n_2}) = N(\pi_1^{n_1}\pi_2^{n_2})$ elements. Therefore, $\mathbb{Z}[i]/\langle\beta_1\beta_2\rangle$ has $N(\beta_1\beta_2) = N(\pi_1^{n_1}\pi_2^{n_2})$ elements. By induction we see that $\mathbb{Z}[i]/\langle\beta\rangle$ has $N(\beta)$ elements for $\beta = \pi_1^{n_1}\pi_2^{n_2}\cdots\pi_s^{n_s}$, where the π_i are distinct Gaussian primes and $n_i \in \mathbb{Z}^+$ for $1 \leq i \leq s$. $\square$

We are now able to construct the set S which plays a crucial role in Gauss's Lemma (Lemma 14). We assume that β is a fixed odd Gaussian integer. By Proposition 2 we know that the number of nonzero congruence classes modulo $\langle\beta\rangle$ is $N(\beta) - 1$. Given that β is odd we know that $N(\beta) > 1$ and also that $N(\beta) \equiv 1 \pmod 4$ since the norm of every odd Gaussian prime is congruent to 1 modulo 4 (see cases 2 and 3 in the proof of Theorem 12). We will partition the nonzero congruence classes modulo $\langle\beta\rangle$ into $(N(\beta) - 1)/2$ orbits, where each orbit contains two distinct congruence classes modulo $\langle\beta\rangle$. Begin by partitioning the units of $\mathbb{Z}[i]$ into the two orbits $\{1, -1\}$ and $\{i, -i\}$. We claim that $1, -1$ are in different classes modulo $\langle\beta\rangle$ and $i, -i$ are in different classes modulo $\langle\beta\rangle$. Assume by way of contradiction that 1 and -1 were in the same congruence class modulo $\langle\beta\rangle$. This means that the difference $1 - (-1) = 2$ would be divisible by β. This would mean that there would exist $\gamma \in \mathbb{Z}[i]$ such that $\beta\gamma = 2$. By taking the norm of the both sides we have $N(\beta)N(\gamma) = 4$ which implies $N(\beta) \mid 4$. This is a contradiction since, by assumption, $N(\beta) \geq 5$ and $5 \nmid 4$. Therefore, 1 and -1 are in different congruence classes modulo

$\langle\beta\rangle$. The same contradiction can be found when looking at i and $-i$.

If $N(\beta) = 5$, then there are two orbits and we are done. If $N(\beta) > 5$, take $\rho_2 \in \mathbb{Z}[i]$ such that $\beta \nmid \rho_2$ and ρ_2 is not in the same congruence class as $1, -1, i$, or $-i$ modulo $\langle\beta\rangle$. This adds two new orbits $\{\rho_2, -\rho_2\}$ and $\{i\rho_2, -i\rho_2\}$. If $N(\beta) = 9$, then there are 4 orbits, and we are done. If $N(\beta) > 9$, then take $\rho_3 \in \mathbb{Z}[i]$ such that $\beta \nmid \rho_3$ and ρ_3 is not in any of the previous congruence classes modulo $\langle\beta\rangle$. This adds two new orbits $\{\rho_3, -\rho_3\}$ and $\{i\rho_3, -i\rho_3\}$. Continue with this process until all nonzero congruence classes modulo $\langle\beta\rangle$ have been exhausted, which leaves $(N(\beta) - 1)/2$ orbits each containing two distinct congruence classes modulo $\langle\beta\rangle$.

We build the set S by choosing one element from each orbit. For convenience, we make the choice $S = \{\tau_1 = 1, \tau_2 = i, \tau_3 = \rho_2, \tau_4 = i\rho_2, ..., \tau_{2m} = i\rho_m\}$ where $m = (N(\beta) - 1)/4$. Now, choose a fixed $\kappa \in \mathbb{Z}[i]$ which is relatively prime to β. If we multiply both elements of an oribt by κ, the two resulting numbers are congruent to the two distinct elements in some (possibly the same) orbit modulo $\langle\beta\rangle$. Because of this, we say that κ takes one orbit to another via multiplication.

We want to show that multiplication by κ permutes the orbits among themselves. Suppose, by way of contradiction, that $\kappa\tau_i \equiv \pm\kappa\tau_j \pmod{\beta}$ for some $i, j \in \mathbb{Z}$ with $i \neq j$. Since $(\kappa, \beta) = 1$, there exists $\gamma, \delta \in \mathbb{Z}[i]$ such that $\gamma\kappa + \delta\beta = 1$. This means that $\beta \mid \gamma\kappa - 1$, so $\gamma\kappa \equiv 1 \pmod{\beta}$. Therefore, κ has a multiplicative inverse γ modulo $\langle\beta\rangle$. By multiplying both sides of $\kappa\tau_i \equiv \pm\kappa\tau_j \pmod{\beta}$ by γ, we have $\tau_i \equiv \pm\tau_j \pmod{\beta}$ which is a contradiction since τ_i and τ_j were taken from two different orbits by assumption. If $\kappa\tau_j \equiv (-1)^{b(j)}\tau_{l(j)} \pmod{\beta}$ for $j = 1, 2, ..., 2m$ and $b(j) = 0$ or 1, this implies that the map $l : \{1, 2, ..., 2m\} \to \{1, 2, ..., 2m\}$ is a bijection. Let $\left\{\frac{\kappa}{\beta}\right\} = \prod_{j=1}^{2m} (-1)^{b(j)}$ and note that $\left\{\frac{\kappa}{\beta}\right\}$ is the same no matter how S is chosen. The proof for this statement is the same as that given for the rational integers at the end of Chapter 2.

It can be proved in general that $\left\{\frac{\kappa}{\beta}\right\} = \left[\frac{\kappa}{\beta}\right]$. We will prove here that $\left\{\frac{\kappa}{\pi}\right\} = \left[\frac{\kappa}{\pi}\right]$ when π is an odd Gaussian prime. Multiply κ by each τ_j for $1 \leq j \leq 2m$ to get the following congruences:

$$\kappa\tau_1 \equiv (-1)^{b(1)}\tau_{l(1)} \pmod{\pi}$$

$$\kappa\tau_2 \equiv (-1)^{b(2)}\tau_{l(2)} \pmod{\pi}$$

$$\cdot$$

$$\kappa\tau_{2m} \equiv (-1)^{b(2m)}\tau_{l(2m)} \pmod{\pi}$$

Since the map $l : \{1, 2, ..., 2m\} \to \{1, 2, ..., 2m\}$ is a bijection, when we multiply these congruences together we are left with the congruence

$$\tau_1\tau_2\tau_3\cdots\tau_{2m}\kappa^{2m} \equiv \tau_1\tau_2\tau_3\cdots\tau_{2m}\prod_{j=1}^{2m}(-1)^{b(j)} \pmod{\pi}.$$

Since each τ_j for $1 \leq j \leq 2m$ is relatively prime to π, we may cancel them all to obtain $\kappa^{2m} \equiv \prod_{j=1}^{2m}(-1)^{b(j)} \pmod{\pi}$. Since $m = (N(\pi) - 1)/4$, then $\kappa^{2m} = \kappa^{(N(\pi)-1)/2}$. From Theorem 13, we know that $\left[\frac{\kappa}{\pi}\right] \equiv \kappa^{(N(\pi)-1)/2} \equiv \prod_{j=1}^{2m}(-1)^{b(j)} \equiv \left\{\frac{\kappa}{\pi}\right\} \pmod{\pi}$. The two symbols $\left[\frac{\kappa}{\pi}\right]$ and $\left\{\frac{\kappa}{\pi}\right\}$ only take on the values of 1 or -1. We claim that the congruence just proved actually implies the equality $\left\{\frac{\kappa}{\pi}\right\} = \left[\frac{\kappa}{\pi}\right]$. Assume, on the contrary, that $\left\{\frac{\kappa}{\pi}\right\} \neq \left[\frac{\kappa}{\pi}\right]$. Then $\pi\gamma = \pm 2$ for some $\gamma \in \mathbb{Z}[i]$. This means that $N(\pi)N(\gamma) = 4$ which is a contradiction since π is an odd Gaussian prime meaning that $N(\pi) \nmid 4$. Therefore, $\left\{\frac{\kappa}{\pi}\right\} = \left[\frac{\kappa}{\pi}\right]$.

An example of the above result is as follows: Let $\kappa = 2 + 3i$ and $\pi = 3$. The orbits modulo 3 are $\{1, 2\}, \{i, 2i\}, \{1 + i, 2 + 2i\}$, and $\{2 + i, 1 + 2i\}$. Let $S = \{1, i, 1 + i, 2 + i\}$. The first congruence shows that $b(j) = 1$, since $(2 +$

$3i)(1) = 2+3i \equiv 2 \pmod 3$. The second congruence shows that $b(j) = 1$, since $(2+3i)(i) = 2i - 3 \equiv 2i \pmod 3$. The third congruence shows that $b(j) = 1$, since $(2+3i)(1+i) = -1+5i \equiv 2+2i \pmod 3$. The final congruence shows that $b(j) = 1$, since $(2+3i)(2+i) = 1+8i \equiv 1+2i \pmod 3$. Therefore, $\left\{\frac{2+3i}{3}\right\} = (-1)(-1)(-1)(-1) = 1$. By equation (3.4), $\left[\frac{2+3i}{3}\right] = \left(\frac{4+9}{3}\right) = \left(\frac{13}{3}\right)$. By part 3 of Theorem 6, $\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$. Therefore, $\left[\frac{2+3i}{3}\right] = 1$ and so $\left[\frac{2+3i}{3}\right] = \left\{\frac{2+3i}{3}\right\}$.

The case where β is an odd Gaussian integer which is not a Gaussian prime is more complicated and the proof will not be given in this thesis. This concludes the construction of Gauss's Lemma in the Gaussian integers.

BIBLIOGRAPHY

[1] A. Adler and J. Coury, *The Theory of Numbers*, Jones and Bartlett Publishers, Boston, 1995.

[2] A. Knoebel, K. Laubenbacher, J. Ludder, and D. Pengellery, *Mathematical Masterpieces: further chronicles by the explorers*, Springer-Vertag, New York, 2007, pp.229-310.

[3] B. Tangedal, Eisenstein's Lemma and Quadratic Reciprocity for Jacobi Symbols, *Mathematics Magazine*, Vol. 73, No. 2, (2000), 130-134.

[4] B. Tangedal, *Eisenstein's Trigonometric Proof of Quadratic Reciprocity*, Unpublished Notes, UNCG, 2009.

[5] B. Tangedal, *Gauss's Lemma in the Gaussian integers*, Unpublished Notes, UNCG, 2010.

[6] D. Rowe, Gauss, Dirichlet, and the Law of Biquadratic Reciprocity, *The Mathematical Intelligencer*, Vol. 10, No. 2, (1988), 13-25.

[7] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag, 1981, pp. 165-166.

[8] James Strayer, *Elementary Number Theory*, Waveland Press, Long Grove, IL, 1994.

[9] P. G. Lejeune-Dirichlet, Recherches sur les formes quadratiques à coefficients et à indéterminées complexes, *Journal für die reine und angewandte Mathematik*, Vol. 24, (1842), 291-371.

[10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd Ed., Springer-Verlag, 1990.

[11] S. Alaca and K. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, Cambridge, 2004.

[12] G. Eisenstein, Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste, *Journal für die reine und angewandte Mathematik*, Vol. 28, (1844), 246-248.

[13] G. Eisenstein, Applications de l'Algèbre à l'Arithmétique transcendante, *Journal für die reine und angewandte Mathematik*, Vol. 29, (1845), 177-184.